
# KISII UNIVERSITY

## Information and Communication Technology Policy

AUGUST, 2014

Kisii University,
P.O.Box 408-40200, Kisii, Kenya
info@kisiiuniversity.ac.ke, www.kisiiuniversity.ac.ke

## VISION

A world-class University in the advancement of academic excellence, research and social welfare

## MISSION

To train human resource that meets the development needs of the country and international labour market, sustain production of quality and relevant research; disseminate Knowledge, Skills, Values and Competencies for the advancement of humanity

## CORE VALUES

Professionalism, teamwork, accountability, responsiveness, integrity

## DEFINITIONS OF TERMS

**Spam**

Unauthorized and/or unsolicited electronic mass mailings

**"Chain letters," "Ponzi," "pyramid" schemes**

Messages that purport to tell the addressee how, for a relatively small investment, the addressee can make huge amounts of money. There are several variations, but they are all based on a common fraudulent

**Port scanning**

It is a process of attempting to learn about the weaknesses of a computer or a network device by repeatedly probing it with a series of requests for information.

**Network sniffing**

This is the process of attaching a device or a program to a network to monitor and record data traveling between computers on the network.

**Spoofing**

This is a deliberate inducement of a user or a computer device to take an incorrect action by Impersonating, mimicking, or masquerading as a legitimate source.

**Denial of service**

Procedures or actions that can prevent a system from servicing normal and legitimate requests as expected.

**Ping attack**

A form of a denial of service attack, where a system on a network gets "pinged," that is, receives a echo-request, by another system at a fast repeating rate thus tying up the computer so no one else can contact it. General use and ownership policy

**User**

The term "User" refers to any person authorized to use University ICT facilities

## ABBREVIATIONS AND ACRONYMS

| | |
|---|---|
| **ICT** | Information Communication and Technology |
| **KSU** | Kisii University |
| **LAN** | Local Area Network |
| **MIS** | Management Information System |
| **WAN** | Wide Area Network |
| **POC** | Point of contact |
| **UPS** | Uninterrupted power supply |
| **ICTC** | Information Communication and Technology Committee |
| **ICTD** | Information Communication and Technology Department |

# TABLE OF CONTENTS

## PREFACE

The vision of Kisii University is to be a World Class University in the advancement of academic excellence, research, and social Welfare. Guided by this vision, the University has strategically positioned itself to train human resource that meets the development needs of the country and the international labour market, and has sustained the production of quality research, dissemination of knowledge, skills and competencies for the advancement of humanity. Information Communication & Technologies *(*ICT*)* plays a vital role in achieving the University's vision and mission. The use of ICT in appropriate contexts can enhance teaching, learning and research by adding different dimensions that was not previously available. ICT may also be a significant motivational factor in students' learning, and can support students' engagement with collaborative learning.

Information Communication &Technology Committee (ICTC) on behalf of the university has taken the mandate of developing an ICT policy. This blueprint will act as a guide in the effective use of ICT resources in the University. The ICT policy framework spells out the principles and goals intended to govern the development, implementation, adoption, monitoring, evaluation and application of Information Communication Technologies (ICTs) in Kisii University. This policy will provide the rationale and philosophy to guide the planning, development and utilization of ICTs in Kisii University. ICTs are always evolving and have contributed immensely to economic, political, social, scientific and educational development in every society where they are deployed. It is the existence and utilization of appropriate ICT policy that would enable individuals, institutions, organizations, nations, or regions to benefit from the developments propelled by the application of ICTs.

**Prof. John S.Akama, PhD**
**Vice Chancellor, Kisii University**

## 1.0 INTRODUCTION

In reference to the Kisii University vision and mission towards becoming a world class University, Information Communication &Technology Department (ICTD) is geared towards becoming a hub of Information Communication &Technology (ICT) infrastructure with sustainable research, learning, development and enhancement of computer literacy that meet the changing needs of the university. Information Communication &Technology Committee (ICTC) on behalf of the university has taken the mandate of developing a blueprint that will act as a guide in the effective use of ICT resources in the University. The ICTC is established by The KSU Statutes 2013 in particular STATUTE XXXV. The ICTC is Chaired by the Deputy Vice-Chancellor (Academic and Student Affairs) with the Director, ICT as secretary.

The ICT Committee shall:

i) prepare, oversee implementation and review the University ICT Policy and align it with the University Strategic Plan;
ii) integrate use of ICTs in teaching, learning and research;
iii) ensure that the University ICT resources are aligned to its stated strategic aspirations;
iv) oversee development and support of major ICT systems and functions;
v) develop and review practice to ensure management and application of University ICT resources is efficient and effective;
vi) assess and advice the University Management Board and Senate on any proposed changes to the current ICT technologies and practices;
vii) ensure that e-learning and teaching is practiced in all Departments, Faculties, Schools and Institutes of the University;
viii) consider and recommend ICT budget and the allocation of ICT resources among users;
ix) facilitate implementation of ICT projects;
x) ensure regular update of the University website, and that the content is relevant;
xi) ensure that ICT investment priorities are effectively aligned with University strategic plan; and
xii) address any other ICT strategic and policy matters as may be referred to it by the University Management Board or Senate.

This policy shall be housed and implemented by the ICTD.

### 1.1 Vision and Mission of ICT Department

#### i) Vision

To become a hub of ICT infrastructure with sustainable research, learning, development and enhancement of computer literacy that meet the changing needs of the university

#### ii) Mission

To develop, deploy and support quality ICT solutions by ensuring availability of efficient and reliable ICT services within the university.

### 1.2 ICT Policy Objectives

i) To serve as the direction pointer for the ICTD's mandate in supporting users, empowering them towards making maximum use of ICT services and resources and specifying the necessary approaches.
ii) To provide guidance in developing a pervasive, reliable and secure communications infrastructure conforming to recognized International standards supporting all services in line with the priorities of the University.
iii) To develop a regulatory framework for ICT related issues.
iv) To establish information and implement security requirements across the University's ICT infrastructure.
v) To uphold the integrity and image of the University through defined standards and guidelines for ensuring that the content of the University's websites is accurate, consistent and up-to-date.
vi) To outline the rules and guidelines that ensure users' PCs and other hardware are in serviceable order, specifying best practices and approaches for preventing failure.
vii) To guide the process of enhancing user utilization of ICT resources through training

### 1.3 Scope of the University ICT Policy

This policy shall be the reference document on ICT standards for Kisii University staff students and any person accessing /developing/implementing and/or using ICT-based

information and resources owned by the University. This Policy applies to all ICT equipment, software or other facilities that is owned or leased by the University

This policy will address the following areas but not limited to:

i) ICT Usage Policy
ii) ICT Security & Internet Policy
iii) ICT Maintenance Policy
iv) ICT Procurement Policy
v) ICT e-Learning Policy
vi) ICT Training Policy.
vii) ICT Disposal Policy

## 2.0 ICT Usage Policy

### 2.1 Overview

The ICT Usage Policy informs the University's staff, students, and other individuals entitled to use University facilities, of the regulations relating to the use of Information Communications Technology systems

ICT facilities are defined to be computing equipment, communications equipment and software applications provided to support the learning, teaching, research, and administrative activities of the University.

It is important that all users exercise a duty of care over their use of ICT facilities; ensuring they are used in a manner that is appropriate; and in ways that will not jeopardize the ability of other users to access ICT resources.

### 2.2 The Policy

The University requires that all people exercise due care and attention over the use of ICT facilities. This applies to the direct (University facilities) and indirect (third party equipment connected to University facilities) use of University ICT facilities.

All users shall comply with the rules below;

2.2.1 All software on any equipment connected to University ICT facilities shall be properly licensed and the terms of the licence be strictly observed.

2.2.2 Users will not access, interfere or remove any ICT facility or data or information unless they have been authorised to so do.

2.2.3 Users shall use ICT facilities in a manner that is consistent with their role.

2.2.4 All use of ICT facilities shall be lawful, honest and decent and shall have regard to the rights and sensitivities of other people.

2.2.5 Users shall not deliberately create, use or distribute materials that could bring the University into dispute.

2.2.6 Duly authorised officers of the University may access or monitor electronic data held on or transiting University ICT facilities where there is a belief that the individual many be in breach of University regulations or the law, or where required to do so by an external agency, e.g. the Police, or where individuals are absent and no arrangements have been made to allow access to information crucial to the working of the University.

2.2.7 Use of computer resources is a privilege and not a right. This privilege can be withdrawn at any time without notice to any user found violating this policy.

2.2.8 Users shall not to install, email, transmit or otherwise make available any material that contains software viruses, confidential information, or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware.

2.2.9 Users shall refrain from any activities that intentionally comprises the computer operating system's security.

2.2.10 Users shall refrain from transmitting, posting or otherwise displaying threatening materials, obscene, discriminatory, or defamatory.

2.2.11 The Administration in consultation with the ICTD reserves the right to determine what type of content can be stored on the computing resources

2.2.12 No equipment may be attached to the network without explicit permission of the ICTD

2.2.13 The ICTD shall protect the University's network and the mission-critical University data and systems.

2.2.14 The ICTD shall not guarantee protection of personal data residing on University ICT infrastructure.

2.2.15 Users shall exercise good judgment regarding the reasonableness of personal use of ICT services. They shall be guided by ICT policies concerning personal use of Internet, Intranet or Extranet systems. In the absence of or uncertainty in such policies or uncertainty, they shall consult the relevant ICT staff.

## 3.0 ICT Security & Internet Policy

### 3.1 Overview

This ICT Policy outlines the acceptable use of ICT equipment and services at the University. The intention of this policy is to promote the University's established culture of openness, trust and integrity. This policy provides the general guidelines on what can be done, and what should not be done, on the University ICT Infrastructure in order to protect ICT resources from injurious actions, including virus attacks, data loss, unauthorized access, network and system failures, and legal problems.

### 3.2 General use

#### 3.2.1 Securing confidential and proprietary information

(a) University data contained in ICT systems shall be classified as either confidential or non-confidential.

(b) Users shall keep passwords secure and shall not share accounts.

(c) All computers shall be secured with passwords.

(d) All hosts connected to the University Internet, intranet or extranet, whether owned by the user or the University shall at all times be required to execute approved virus-scanning software with a current virus database.

(e) The user shall exercise caution when opening e-mail attachments received from unknown senders, which may contain viruses.

#### 3.2.2 Unacceptable use

(a) Under no circumstances shall an employee, student, contractor or any staff be authorized to engage in any activity that is illegal under Kenyan or international law while utilizing the University ICT resources.

(b) The following activities shall be prohibited with no exceptions:

**i)** Violation of the rights of any person or company protected by Kenya's copyright, trade mark, patent, or other intellectual property (IP) law and the University's Intellectual Property Policy, other relevant policies, or the University's code of conduct.

**ii)** Introduction of malicious programs into the network or server, for instance viruses, worms, Trojan horses or e-mail bombs.

**iii)** Sharing of the University user accounts and passwords– users shall take full responsibility for any abuse of shared accounts

**iv)** Using the University computing resources to actively engage in procuring or transmitting material that could amount to sexual harassment or constitute creation of a hostile work environment.

**v)** Making fraudulent offers of products, items, or services originating from any the University account.

**vi)** Causing a security breach or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which one is not an intended recipient or logging onto a server that one is not expressly authorized to access, unless this is within the scope of regular duties.

### 3.3 Password Policy

Computer passwords are used for various purposes at the University according to the set rules.

#### 3.3.1 Password rules

(a) All system-level passwords such as root, administrator, shall be changed twice a month.

(b) All user-level passwords such as email, web, and desktop computer shall be changed at least once every three months.

(c) Passwords shall not be inserted into email messages or other forms of electronic communication.

(d) All passwords shall be treated as sensitive & confidential.

(e) Where an account or password is suspected to be compromised the affected passwords shall be changed immediately.

(f) All user-level and system-level passwords shall conform to the guidelines described below. The password shall:

i) Contain at least eight characters
ii) Not be a word found in an English, Swahili or other dictionary
iii) Contain both upper and lower case characters like a-z, A-Z.
iv) Have special characters, digits as well as letters.
v) Not be based on personal information, or names of family, among others.

### 3.3.2 Application Password Security

Application developers shall ensure that their programs contain the following security precautions.

(a) Shall support authentication of individual users, not groups.
(b) Shall not store passwords in clear text or in any easily reversible form.
(c) Shall provide for some sort of role management, such that system administrator can take over the functions of another user account without having to know the usesr's password.

## 3.4 Server Security Policy

### 3.4.1 Ownership and Responsibilities

Any server deployed on the University ICT network shall have an operational group that shall be responsible for its system administration. Operational groups shall monitor configuration compliance and shall implement an exception policy tailored to their environment. Each operational group shall establish a process for changing the configuration guides.

### 3.4.2 General configuration guidelines

(a) Server Operating Systems shall be configured in line with approved ICT guidelines.
(b) Access to services shall be logged and protected through access-control methods.
(c) The most recent security patches shall be installed on the systems as soon as practical, the only exception being when immediate application would interfere with business requirements.
(d) Antivirus software shall be installed and configured to update regularly.
(e) User access privileges on a server shall be allocated on “least possible required privilege” terms, just sufficient privilege for one to access or perform the desired function.

(f) Servers shall be physically located in an access-controlled environment.

### 3.4.3 Monitoring

(a) All security-related events on critical or sensitive systems shall be logged and audit trails backed-up in all scheduled system backups.

(b) Security-related events shall be reported to the ICTD for corrective measures as needed.

## 3.5 Internal Computer Laboratory security policy

### 3.5.1 Ownership responsibilities

(a) ICTD shall appoint officers, designated as Computer Laboratory administrators, who shall take charge of their computer laboratories. A Computer Laboratory administrator shall be responsible for the day to day running of a Computer Laboratory, and shall be the point of contact (POC) for the ICTD on all operational issues regarding the Laboratory.

(b) Computer Laboratory administrators shall be responsible for the Laboratory's compliance with all the University ICT policies.

(c) Computer Laboratory administrators shall be responsible for controlling access to their computer laboratories

(d) The ICTD reserves the right to interrupt laboratory connections if such connections are viewed to impact negatively on the ICT infrastructure, or pose a security risk.

### 3.5.2 General configuration requirements

(a) Computer laboratory network devices (including wireless) shall not cross-connect a laboratory to a production network.

(b) Computer laboratories shall be prohibited from engaging in port scanning, network auto-discovery, traffic spamming or flooding, and similar activities that may negatively impact on the overall health of the University network and/or any other network.

(c) In computer laboratories where non-University users are allowed access (such as computer training laboratories), direct connectivity to the University production network from such laboratories shall be prohibited.

(d) No University confidential information shall reside on any computing equipment located in the laboratories.

### 3.6 Anti-virus policy

(a) All Computers connected to the University ICT network shall run the University standard supported anti-virus software, and shall be configured to perform daily full-system and on-access scans.

(b) Anti-virus software and the virus pattern files shall be kept up-to-date always through scheduled daily automatic updates.

(c) Computer laboratory administrators and owners of computers, in consultation with the relevant ICTD personnel, shall be responsible for executing required procedures that ensure virus protection on their computers.

(d) Once discovered, any virus-infected computer shall be removed from the University network until it is verified as virus-free.

### 3.7 Physical Security policy

#### 3.7.1 Required physical security

(a) All University hardware shall be prominently marked, either by branding or etching.

(b) All personal computers (PCs) fitted with locking cases shall be kept locked at all times.

(c) Wherever possible, computer equipment shall be kept at least 1.5 metres away from external windows in high-risk situations.

(d) All opening windows on external elevations in high-risk situations shall be fitted with permanent grills.

(e) All external windows to rooms containing computer equipment at ground floor level or otherwise visible to the public shall be fitted with window blinds or obscure filming.

(f) All doors giving access to the room or area with computer equipment from outside the building shall be fitted with supplementary metal grills.

#### 3.7.2 Computer server rooms

(a) Computer servers shall be housed in a room built and secured for the purpose.

(b) The computer server rooms shall contain an adequate air conditioning system in order to provide a stable operating environment and to reduce the risk of system crashes due to component failure.

(c) No water, rainwater or drainage pipes shall run within or above computer server rooms to reduce the risk of flooding.

(d) Where possible the floor within the computer suite shall be a raised false floor to allow computer cables to run beneath the floor and reduce the risk of damage to computer equipment in the case of flooding.

(e) Power feeds to the servers shall be connected through uninterrupted power supply (UPS) and surge protector equipment to allow the smooth shutdown and protection of computer systems in case of power failure.

(f) Where possible generator power shall be provided to the computer suite to help protect the computer systems in the case of a mains power failure.

(g) Access to the computer server rooms shall be restricted the authorized University staff only.

(h) All non-ICTD staff working within the computer server room shall be supervised at all times and the ICT management shall be notified of their presence and provided with details of all work to be carried out, at least 24 hours in advance of its commencement.

### 3.7.3 Access control

(a) The system Administrator in charge of a particular system shall be the only authorized person to assign system, network or server passwords for relevant access to the system.

(b) The system administrator shall be responsible for maintaining the integrity of the system and data, and for determining end-user access rights.

(c) All supervisor passwords of vital network equipment and of those critical University servers shall be recorded in confidence in case of emergencies.

(d) System audit facilities shall be enabled on all systems to record all log-in attempts and failures, and to track changes made to systems.

### 3.7.4 Physical LAN/WAN security

(a) Switches

i) LAN and WAN equipment such as switches, hubs, routers, and firewall shall be kept in secured rooms. In addition, the equipment shall be stored in lockable air-conditioned communication cabinets.

ii) All communication cabinets shall be kept locked at all times and access restricted to relevant ICT staff only.

iii) Whenever legitimate access to communication cabinets is necessary, it shall be done with physical supervision of the responsible ICT personnel.

(b) Workstations

i) Users shall log out of their workstations when they leave their workstation for any length of time.

ii) All unused workstations shall be switched off outside working hours.

(c) Servers

i) All servers shall be kept securely under lock and key.

ii) Access to the system console and server disk or tape drives of the production servers shall be restricted to authorized ICTD staff only.

(d) Electrical security

i) All servers and workstations shall be fitted with UPS to condition power supply.

ii) All switches, routers, firewalls and critical network equipment shall be fitted with UPS.

iii) Critical servers shall be configured to implement orderly shutdown in the event of a total power failure.

(e) Inventory management

i) ICTD shall maintain an updated inventory of all computer equipment and software in use throughout the University.

ii) Computer hardware and software audits shall be carried out periodically to track unauthorized copies of software and changes to hardware and software configurations.

### 3.8 Backup Policy

Users are responsible for carrying out weekly backups to ensure the recovery of data in the event of failure. These backup provisions will allow University processes to be resumed within a reasonable amount of time with minimal loss of data. Since failures can take many forms, and may occur over time, multiple versions of backups should be maintained.

Backups of all University records and software must be retained such that computer operating systems and applications are fully recoverable. This may be achieved using a combination of image copies, incremental backups, differential backups, transaction logs, or other techniques.

Backup process shall be guided by the following:

i) The frequency of backups is determined by the volatility of data; the retention period for backup copies is determined by the criticality of the data

ii) Backup records must be stored in a secure, off-site location. An off-site location may be in a secure space such as a safe in a separate building. The practice of taking backup media to the personal residence of staff persons is not acceptable

iii) Derived data should be backed up only if restoration is more efficient than creation in the event of failure.

iv) Users will be required to backup data in external storage media weekly.

v) Backup and recovery documentation must be reviewed and updated regularly to account for new technology, business changes, and migration of applications to alternative platforms.

vi) Recovery procedures must be tested on an annual basis.

## 4.0 ICT Procurement Policy

i) ICTD shall provide technical advice for any ICT equipment and software to be purchased by the University and ensure that all items purchased meet the user specification.

ii) All new buildings at Kisii University shall have structured wire cabling. All ICT Network infrastructures shall be in accordance to ISO standards and Communication Commission of Kenya regulations.

## 5.0 ICT Maintenance Policy

The ICT maintenance policy will address all issues concerning proper maintenance and the frequency of this maintenance. Primary maintenance of the ICT resources may be automated however the ICT department shall remain responsible for all maintenance. All the possible points of entry should be addressed by the ICT Security policy. This policy will address both physical and logical security and in order for the policy to work it must be enforceable. The policy will also address timely system backups, and recovery.

## 6.0 ICT e-Learning Policy

In addition to other modes of course delivery, KSU shall have educational provision which is delivered and/or supported and/or assessed through electronic means. This includes e-learning learning, blended learning, instructor led training and the use of web-based materials to supplement classroom-based learning. For the purposes of this Policy these are all simply termed the “e-learning mode”.

6.1 This Policy outlines the minimum requirements that the University expects to be met by schools, campuses, faculties, departments, centres and institutes when delivering under the e-learning mode. The requirements of the policy are in addition to Commission for University Education (CUE) and KSU Academic Quality Assurance mechanisms for course delivery.

6.2 Schools, campuses, faculties, departments, centres and institutes shall ensure that on the e-learning platform:

(a) Information that sets out the respective responsibilities of the University and the learner for delivery under the e-learning mode is available and adequately updated.

(b) Learners have access to module descriptions to show the intended learning outcomes and teaching, learning and assessment methods of the module(s).

(c) Learners have access to clear schedules for the delivery of their study materials and for assessment of their work.

(d) The study materials delivered through e-learning platform meets the expectations of the University in respect of the quality of research, teaching and learning-support material.

(e) Clear and up-to-date information about the learning support available to learners locally and remotely for their programme or elements of study.

(f) Appropriate opportunities to give formal feedback on learners' experience of the programme on e-learning platform.

6.3 Schools, campuses, faculties, departments, centers and institutes, in liaison with the ICT Department, shall ensure that the e-Learning system is secure, reliable and functional in accordance with internationally acceptable standards and KSU's Quality Assurance requirements.

## 7.0 ICT Training Policy

ICTD believes the benefits to be derived from using Information Communication Technology (ICT) within KSU are significant and that every staff and student at KSU should have the opportunity to develop personal ICT competence and to use and extend personal ICT competence in a range of activities.

7.1 It is the intention of this ICT policy to secure the following within KSU:

(a) To identify and maximise the appropriate use of ICT to enrich Students learning and teaching experiences.

(b) To respond positively to new guidance on use of ICT when it arises.

(c) To provide staff and students with the skills, knowledge and understanding to make maximum use of existing ICT resources.

(d) To help KSU staff to incorporate ICT into their administrative and management practice through appropriate training and support.

(e) To ensure that ICT equipment is available in sufficient numbers at suitable sites around the University to enable staff and students at KSU to maximise the real benefits ICT offers to the enhancing of learning and teaching.

7.2 ICT competence shall be achieved by:

i) Developing sufficient skills and expertise amongst staff and students to maximise the appropriate use of ICT.

ii) Developing sufficient ICT resources and maximising the availability of ICT resources to enable access to ICT resources to be a daily reality for students and staff.

### 7.3 ICT Training Resources

The University shall provide the ICT infrastructure for learning, research and general office use as follows:

**(a) Personal Computers**

i) The Computer Lab and Library PCs are 'bookable' resources, via the ICT Lab Attendants in the Computer Laboratory and Library.

ii) The computers allocated for office use shall only be used for the purpose of such allocation.

(b) **Digital Projectors**

Almost all teaching areas in KSU should have a ceiling mounted projector. These are complemented by portable projectors which are available to ensure full coverage across the University.

(c) **Laptops**

All Senior Managers and faculties should have their own dedicated laptops. Furthermore, staff can have access to their departmental/faculty laptops.

## 8.0 ICT Disposal Policies

### 8.1 KSU's Hardware Sanitization Policy

8.1.1 The purpose of KSU's Hardware Sanitization Policy shall be to protect the University intellectual property and the confidentiality of University data residing on all hardware owned or leased by KSU.

8.1.2 This Policy is complementary to any other implemented policies dealing specifically with hardware retention and disposal.

8.1.3 Hardware may not require sanitization if it is transferred internally to another user within the same department. Hardware that is either transferred to a different department or to an employee with less authority must be sanitized in the same way as hardware transferred externally.

8.1.4 All hardware transferred externally must be sanitized according to the methods defined in this Policy. This scenario includes:

(a) hardware transferred to the private ownership of employees or students

(b) hardware donated to charitable organizations

(c) hardware returned to a leasing company

(d) hardware returned to a vendor for servicing or maintenance

(e) Hardware released to an external agency for disposal.

8.1.5 One of the following methods may be used to sanitize hardware:

8.1.5.1 Physical destruction, whereby hardware shall be sanitized through crushing, shredding, incineration, or melting.

8.1.5.2 Digital sanitization. Deleting files is insufficient to sanitize hardware. A digital sanitization tool must be used.

8.1.6 The University shall acquire and use an approved sanitization tool to be managed by the ICT Department in properly sanitizing the hardware. At the end of sanitization, a certification shall be signed as evidence that the equipment has been properly sanitized before it can be supplied, transferred, or donated. Copies of all sanitization certificates shall be kept by the ICT Department.

8.1.7 The ICT Manager is the primary contact on sanitization issues. KSU users should consult with the ICT Department prior to disposing of any computer equipment.

## 8.2 ICT Assets Disposal Policy

8.2.1 KSU's surplus and/or obsolete non-leased ICT assets and resources (i.e. PCs, printers, handheld devices, servers, hubs, network switches, bridges, routers etc.) shall be discarded and disposed of in accordance with standards, procedures, and restrictions established and defined in this Policy, in a cost-effective manner and in compliance with legal requirements and environmental regulations, through appropriate external agents and KSU's upgrade guidelines. All disposal procedures for retired ICT assets must adhere to University-approved methods.

8.2.2 Where applicable, it is desirable to achieve some residual value of the ICT asset in question through reselling, auctioning, donation, or reassignment to a less-critical function.

8.2.3 After sanitization, ICT assets and equipment for disposal shall be handed over to the Assets Disposal Committee for further action.

8.2.4 KSU shall apply from among the following acceptable methods of ICT assets disposal:

(a) sell to existing KSU staff
(b) auction online
(c) sell as scrap to a licensed dealer
(d) use as a trade-in against cost of replacement item
(e) reassign to a less-critical business operation function
(f) donated to schools, charities, and other non-profit organizations
(g) recycle and/or refurbish to leverage further use (within limits of reasonable repair)
(h) discard as rubbish in a landfill after sanitization of toxic materials by approved service provider.

## 9.0 Policy Enforcement

Any KSU staff or student who is found to have violated this ICT Policy may be subject to disciplinary action up to including dismissal and as it may be stipulated in the KSU Student Handbook and Collective Bargain Agreement.

## 10.0 SELECTED REFERENCES


Bradford University ICT Strategy

Catholic University of East Africa (CUEA), ICT Policy, 2013

Jaramogi Oginga Ondinga University of Science and Technology ICT Policy, 2014

Makerere University ICT Policy Master Plan Phase 2 (2005 – 2009)

Maseno University ICT Policy

Murdoch University IT Security Standards and Guidelines

University of Botswana Distance Education Mainstreaming Policy

University of Cape Coast ICT Policy

University of Cape Town Information and Communication Technology Strategy

University of Greenwich Rules and Regulations for Use of ICT

University of Mauritius IT Policy

University of Nairobi ICT Policy

University of Sydney ICT Policy

University of Wales Swansea ICT Strategic Plan 2003 – 2004

University of Westminster Acceptable Use Policy


## 11.0 Policy Approval

**VICE CHANCELLOR** **APPROVAL DATE:** 9TH AUGUST, 2014