University of
Eldoret
flame of knowledge and innovation

INFORMATION & COMMUNICATION TECHNOLOGY POLICY

Version	**1.0**
Short description	Information & Communication Technology Policy
Relevant to	Staff, Students and other Stakeholders
Approved by	University Council
Responsible officer	Director ICT
Responsible office	Office of the Vice-Chancellor
Date introduced	June, 2014
Related university and national documents	University Charter, Statutes; National Information and Communication Technology Policy; Kenya National Library Services ICT Policy and other relevant policies.
Related legislation	Constitution of Kenya, 2010; Universities Act, 2012; The Kenya Information & Communication (Amendment) Act, 2013
Key Words	ICT

JUNE, 2014

APPROVAL

The University of Eldoret having been awarded its Charter on 11th February 2013 has set on a growth path guided by its vision of "being a Premier University that is globally visible in knowledge generation and technological innovation". As part of laying its foundation, the University developed its Statutes in November 2013 followed by its first strategic plan which will be rolled out later this year, 2014.

The process of recruiting its top managers was completed in March 2014. The University has now embarked on the process of developing its policies which will guide decisions of the different organs of the University in order to achieve rational outcomes geared towards the growth of the University. This Information & Communication Technology Policy is just one of the many policies that the University is rolling out.

My special thanks go to all those who put in their time, effort and skills to develop this Policy.

By virtue of the authority vested in me as the Chairman of Council of the University of Eldoret and in reference to the approval granted by Council in its meeting of………………, I hereby sign this Information & Communication Technology Policy this…13th….day of…June…..2014.

Prof. Sarone Ole Sena. B.Ed.; M.Phil.; M.Sc.; Ph.D.
Chairman of Council

Table of Contents

DEFINITIONS AND ACRONYMS

Definitions

Access: This is connection to ICT electronic resources, either directly or indirectly.

Account: A combination of a username and password given to an authorized user (the account owner) to access University's ICT electronic resources (Services, Infrastructure and Facilities).

Algorithm: A code used for encrypting and decrypting data/information using a certain procedure.

Anti-Virus: A computer code, program or software used for detecting and removing known and unknown computer viruses.

Authorized User: A person with permission to access University of Eldoret's electronic resources.

AV equipment: Refers to audio-visual teaching materials or aids, such as digital cameras, video recorders and data projectors etc.

Backup: Making a copy of a file for recovery in case of system failure.

Copyright: A form of intellectual property which gives the creator of an original work exclusive right in relation to that work, and control over its distribution, publication, and adoption.

Device Encryption: This is a method of transforming electronic information using a computer algorithm, thereby making it indecipherable to unauthorized users.

Electronic Resource*:* This includes any file/data/information that is stored in digital format.

Email: Electronic Mail or messages send through an electronic communication methods.

Encryption: This is a security procedure used to convert data from its original format to one that is not easily construed except by the intended user.

Firewall: This is a software and/or a device that controls access by acting as a barrier between two or more parts of a computer network.

Gateways: These are ICT Services where connection to any network device is only through authorization (such as Learning Hubs, the Library or wireless connections).

ICT

***Directorate*:** The Directorate charged with the responsibility of managing and supporting all computers, networks, and telecommunications systems within the University.

ICT facilities/ equipment: Include computer servers, computer terminals, printers, telephones, networks, faxes, on-line and off-line storage media and related equipment, end-host devices, licenses, centrally managed data, computer laboratories, video conference rooms, and any software that is either owned or leased by the University as well as data files that are owned, managed or maintained by UoE. These facilities also include all electronic communication devices, networks, data storage, Infrastructure hardware, and network connections to external resources.

ICT Services: These are systems which support any form of information or communication provision, interaction, or information storage as well as the ICT Facilities which they operate on. They include any communication device or application such as cellular phones, radio, computer, television, servers and hardware or software for the network, satellite systems, and other services and applications related with them, including distance learning and videoconferencing.

Information Systems: This include files, databases, soft-wares such as applications and systems software and hardware assets such as servers, computers, communications equipment, magnetic storage media and other development tools.

Internet: This is an interconnected system of computers or/and computer networks used for sharing information along many channels, and over many protocols.

Intranet: Private network that is established for access by authorized users only.

Mobile Computing: This is the use of portable communication devices such as cell phones, tablets, laptops, or PDA to do computing in a way that is not fixed or at a particular location.

Network Port: Any individual switch port, wall outlet or wireless access port providing connectivity to the University of Eldoret network.

Network: Any data communications links such as Ethernet, fiber, or twisted pair etc that are located at UoE sites or one of its campuses or any connections between these sites.

Password: String of characters used for authentication of a user's identity.

Personal

Files: These are files, records or documents of personal nature, and have no relation with the University or its business.

Port Splitter: These are devices connected to a network port that allows simultaneous access via that port, and they include, but not limited to:

i. Routers;

ii. Switches;

iii. Modems;

iv. Wireless Access Points;

v. HUBS; and

vi. Any other network device having active network connections beyond one.

Remote Access: Ability to access an ICT resource or the UoE network from a location other than being physically at University of Eldoret.

Security: These are measures taken to ensure a reliable computing environment with no risks of loss data.

Server: A computer that stores centralized information/data and issues services or information whenever requested to other computers or devices.

Shared Account: Any UoE ICT account that is accessed by many users

Software: This is a computer program or operating information that is used by, or installed on, or stored on computers owned by the University and other storage media including CDs, Backup tapes, DVDs, CDs and VCDs.

Spam: Unsolicited and/or unauthorized mass electronic mailings.

Student: Anyone who is enrolled for study at the University of Eldoret.

System Administrator: ICT staff responsible for the operation of the system, and who is authorized to determine any user with permissions to access particular ICT resources.

TCP/IP: These are a set of communication protocols used to perform data transfers between computers over the Internet.

University: This refers to University of Eldoret

User: Authorized users who logs in or uses a system, either by direct connection via a modem or network or across one or more networks.

Username: This is a distinct string of characters for authenticating a specific user.

Virus: This is potentially malevolent code that can cause unwanted or unanticipated events in a computer.

Wireless Network: An ICT network that uses electromagnetic waves to transmit data. This is commonly referred to as Wi-Fi, 802.11 or WLAN.

Webmaster: Someone who is responsible for designing, managing, maintaining, and updating the website and web server.

ACRONYMS

CD-ROMS:	Read only memory compact discs

CD-RW:	Read/Write Compact Disc
CDs:	Compact Discs
DNS/DHCP:	Domain Name Server/Domain Host Control Protocol
DVDs:	Digital Video Discs
FTP:	File Transfer Protocol
ICT:	Information and communication Technology
IP:	Internet Protocol
ISO:	International Organization for Standardization
LAN:	Local Area Network
LCD:	Liquid Crystal Display
NFS:	Network File System
OS:	Operating system
SQL:	Structured Query Language
SSH:	Secure Shell
TCP:	Transmission Control Protocol
UoE:	University of Eldoret
UPS:	Uninterruptible Power Supply
VPN:	Virtual Private Networking
WAN:	Wide Area Network
WIFI:	Wireless Fidelity – technology that allows an electronic device to exchange data or connect to the internet using radio waves.
WLAN:	Wireless Local Area Network
WWW:	World Wide Web
ZIP:	Format for compressing files

FORWARD

The **University of Eldoret** is one of the public universities in Kenya. It is situated approximately 9 km along the Eldoret-Ziwa road in Eldoret town, Uasin Gishu County. It was founded in 1946 by the white settlers as a Large Scale Farmers Training Centre. In 1984, it was converted to a teachers' training college and renamed Moi Teachers' Training College to offer Diploma Science Teachers Training. Due to the double intake crisis, the College was taken over by Moi University as a Campus in 1990, renaming it Chepkoilel Campus. From 1990, the University made it a campus of natural, basic and applied science programmes. In August 2010 the President, through Legal Notice No. 125 of 13 August 2010 upgraded the campus into a University College with the name Chepkoilel University College, a Constituent College of Moi University. Upon the award of Charter by the President on February 2013, the University College was renamed **University of Eldoret**.

Although the University of Eldoret supports freedom of expression and an open environment for scholarly research, the contents of this policy document must, also comply with other University guidelines, as well as the Kenyan laws. This document is therefore a guide to ensure that electronic resources are used ethically and responsibly by the University community.

This policy document describes the position of University of Eldoret with regard to how ICT will be used to achieve the University's desired goals and continued excellence, in teaching, research and extension.

Akenga

Prof. Teresa A. O. Akenga, B.Ed., M.Sc., Ph.D., MRSC, MBS
Vice-Chancellor

1.0 INTRODUCTION

1.1 Preamble

In achieving its objectives, mission and vision of providing high quality Education and training in Science, Agriculture and Technology that promotes networking, Partnerships and linkages with other institutions and industry, University of Eldoret has placed ICT as an integral part towards the attainment of these goals and objectives. University of Eldoret prides itself as a premier institution in provision of higher education and will continue to nature its ideals for the benefit of its students, staff, alumni and other stakeholders.

This policy document describes the use of ICT resources by authorized users in the University of Eldoret .

It is the responsibility of every user to understand these guidelines and to carry out their activities accordingly.

The University encourages and supports public-private partnerships in provision of ICT services on mutually agreed terms.

This ICT Policy document has been developed in line with the National ICT policy guidelines and it contains the respective policies, their statements, as well as the governing rules and regulations.

This document may be revised as new situations arise within the UoE, so as to reflect the changes in policies and procedures.

1.2 Information and Communication Technology (ICT) Directorate's responsibilities

The following tasks form the core responsibilities of ICT Directorate with regard to this policy:

(i) To manage and implement the ICT policy;

(ii) To develop procedures for ICT projects within the University and evaluate, whether its appropriate to do internal development or to purchase.

(iii) To establish and maintain good working relationships with suppliers of ICT resources.

(iv) To maintain an inventory of all the installed ICT services/facilities, and to develop the necessary standards for the establishment of:

a. Appropriate Operating systems.

b. Data Documentation processes.

c. Metadata repository or Data dictionary.

d. Standards of communication.

(v) To establish, develop and nurture suitable career progression for ICT staff.

(vi) To assess and review ICT equipment and services to determine the ones that are due for repair, replacement, obsolete or those that may be redesigned.

(vii) To develop suitable training programs for all users.

(viii) To prepare suitable procedures to guide in the acquisition of ICT hardware/software, and to assist users with technical support and management.

1.3 Responsibilities of Users

The following constitute some of the responsibilities of an authorized user of ICT Resources within UoE:

i. They should ensure ethical and responsible use of ICT services, resources and facilities;

ii. They should evaluate their ICT needs and the level of ICT support services needed;

iii. They must report any misuse of ICT services, resources and facilities;

iv. They must asses and appraise their ICT equipments, security and performance regularly;

v. They must ensure that they understand these policies and propose any changes according to their requirements;

Users also need to be aware that all activities involving personal use of the University's ICT resources must not cause offense to other users, or be considered on rational terms to offend, or disrupt other users or deter persons carrying out University work from accessing ICT Facilities and Services.

1.4 Senior management roles

Any success of implementing these ICT policies depends on the support given by top University management with regard to development, implementation and enforcement since it impacts both directly and indirectly on all planning and day-to-day operations of the University. It is therefore important that management understands these policies so that the University's goals and objectives are clearly tied with these ICT policies.

1.5 Responsibilities regarding ICT Policy Planning

All stakeholders within the University such as the Academics Division, Administration, Library and the ICT directorate are expected to participate in the planning process of ICT activities within the University. Good and strategic planning ensures that the ICT policies put in place support the operations and functioning of the University.

1.6 Other Responsibilities

i) There shall be an ICT committee/board which shall have the overall responsibility of reviewing and ensuring approval of all ICT-related policies. The committee shall be constituted as per the University statutes.

ii) The ICT Director shall oversee the overall strategic direction, management and operation of the University's ICT infrastructure and services, in line with the strategic and operational objectives of the University. As the designated information security owner, the ICT Director has overall responsibility for Information security, its governance framework and ensuring that all sectors of the University implement the relevant policy.

iii) The ICT staff have the responsibility of undertaking regular risk reviews to ensuring that all risks are carefully established and that all realistic measures are taken to avert any security incidences.

iv) All system Owners shall have the responsibility over a given application, service, data process or infrastructure facility.

v) System Administrator(s) shall be responsible for the security and integrity of all ICT infrastructures in the University and its Campuses as well as other ICT facilities and services.

1.7 University integrated information Systems

With increasing number of users, there is need to collect data at a central point for access by many users and also to develop adequate networks which are secure, reliable and also guaranteeing privacy to users. University of Eldoret recognized the need for an integrated information system and has thus put in place a student management information system, a financial management information system, an asset management and a procurement information system among others. These systems together with their use shall be governed by these policies.

In implementing ICT services and information systems within the University, the nature and the relationship between the different ICT systems and services shall be taken into account. For example, a student's management information System may only be accessed by remote users if suitable connectivity within the University and the LANs are established between the central database server containing the students Records and the remotely located user's computers.

1.8 Inspection of Computers

In safe guarding the security of the University's network and facilities, computers may be inspected whenever a breach is detected or suspected. Only the Vice Chancellor has this authority through the ICT Directorate, and disclosure of any information to an external organization shall only be possible upon the production of a relevant legal document.

System Administrators or other authorized staff may monitor equipment, systems, computers, servers, and network traffic at any time so as to preserve the security and the integrity of the network as per these policies. In case of system maintenance, all data and other transmissions may be monitored, viewed and analyzed. The University shall have the right to audit networks and systems from time to time, in order to ensure full compliance with these policies.

1.9 Limitations

The ICT policy set out in this document does not cover specialized applications used in teaching processes such as Computer Aided Learning and professional applications to be used in specific educational and scientific fields. The policy does not also include provision of specific applications for research purposes as these shall be the responsibility of the Schools/Departments concerned. The University ICT policy will however ensure that, all end users are equipped with the necessary level and various ICT skills to assist their functions.

1.10 Purpose of the Policy

This policy is intended to:

i. Streamline the operations and use of the University's ICT resources and services in line with the vision and mission of University of Eldoret.

ii. Help the University's management and other decision-makers in making short, medium and long term strategic decisions on operations of the University.

iii. Be a guiding document to management in relation to all ICT related developments and decisions.

This ICT Policy document has been developed on the basis of a detailed feasibility study and a University-wide needs analysis that is supported by careful decision making by the University management. The ICT Policies, by virtue of their approval by the University Council, may be considered as the principal guide of structured ICT resources and services planning, their implementation and decision making.

Like all other resources within UoE such as staffing etc, ICT resources, services and systems require careful planning, controlling, monitoring processes, and staffing levels. Consequently, the development of ICT policies within the areas of operations of the University has become key.

1.11 Objectives of the Policy

The objectives of the ICT policy are:

i) To ensure optimum use of all University ICT services and facilities.

ii) To facilitate adherence to information security features of ICT by all users;

iii) To ensure that all University computing facilities and services are not misused, abused or any data lost;

iv) To facilitate compliance with Information Security ISO standard wherever possible;

v) To create awareness for all users of their responsibilities for the protection and security of the ICT resources which they control;

vi) To ensure sufficient awareness is created for appropriate information and physical security measures to be put in place for the optimal operation and support of ICT facilities and services;

vii) To facilitate full compliance of all users of these policies, processes and any other relevant laws;

1.12 Non-compliance

Any breach or violation of this policy will result into disciplinary measures being taken as contained in the relevant University statutes and/or employer-staff agreements.

1.13 Scope of the ICT Policy

This policy covers all staff of UoE (including casual staff), bonafide students and visitors who are allowed access to the University's ICT resources and it must be read together with all other university policies. It also applies to (but not limited to):

i. All users who have signed up for internet connection within their hostels.

ii. All users of Mobile Devices who perform University business on such a Device, in spite of whether they own it or it belongs to the University.

iii. All users of UoE Email services and the related facilities.

iv. All users of ICT services at University of Eldoret & providers of ICT equipment and services in the University and all related parties including staff and students at collaborating institutions who access UoE ICT systems and services.

v. All UoE users who use Social Networking Sites.

These policies also govern persons using UoE's ICT Systems, on privately owned devices that are not managed or maintained by UoE.

1.14 Policy Provisions

University of Eldoret shall provide ICT Resources and Services (Facilities and Infrastructure) to support its key objectives of learning, teaching, research and other day-to-day operations.

The University provides public services and/or private services, which are available to Authorized Users only, who hold an active account. At the end of their agreed affiliation with the University, they shall cease to be considered as Authorized Users and their Access shall be terminated.

The Public services include, but are not limited to, the University’s web site and the information contained on it and other services offered by the University Library.

All other services are private and are provided by the University of Eldoret to Authorized Users only.

2.0 ICT Administrative and Operational Structures

The management of ICT shall operate in three levels namely, the Vice-Chancellor, The ICT Director, and the ICT management board/committee together with School representatives.

i) The Vice-Chancellor shall be responsible for the overall leadership of the University's ICT, Infrastructure, Facilities and Services.

ii) The ICT Director shall determine the overall direction of Information, Communication and Technology within the University, as per the university statutes and as stated elsewhere in this policy.

iii) The ICT Management Board/Committee and School representatives shall advice on University-wide ICT policies, and all matters constituting ICT infrastructure in collaboration with the ICT Director who shall in turn, advice the Vice-Chancellor on such matters.

2.0.1 Director, ICT Directorate

The head of the ICT Directorate shall be a Director whose rank shall be that of Senior lecturer and above, and who shall be appointed as per the University statutes, rules and regulations. He/she shall report directly to the Vice-Chancellor and whose management tasks shall include but not limited to;-

i. Coordination of University-wide information system planning, utilization and performance evaluation;

ii. Operational responsibility for central processing and data communication systems;

iii. Establishment and enforcement of standards and the ICT policy guidelines for the University-wide applications, databases and communication network;

iv. Implementation of ICT projects within the University of Eldoret;

v. Planning and control of ICT services provided to external parties;

vi. Managing Information security and other functions/duties as per other sections of this policy document;

vii. Maintaining the organizational and human resource infrastructure for technical services and assistance to all organizational units.

2.0.2 Deputy Director-Maintenance and Operations

The Deputy Director (Maintenance & Operations) shall be appointed as per the University establishment and employment procedures, and he/she oversee the operations of the following units:-

i. ICT Planning and Development

ii. Systems administration

iii. Web Development

iv. Overall Maintenance, Repairs and Operations as well as other responsibilities as indicated elsewhere in this policy document.

2.0.3 Deputy Director-Information Systems Support

The Deputy Director (Information Systems Support) shall be appointed as per the University establishment and employment procedures, and he/she Shall be responsible for the operations of the following units:-

i. Database Administration

ii. Open and Distance Learning program (ODEL)

iii. Information Systems Support

iv. ICT Training and other responsibilities as indicated elsewhere in this policy document.

2.1 ICT Planning and Development unit

This unit shall be responsible for:

i. Acquisition and dissemination of knowledge (expertise on advanced technologies and innovative application of ICT at University of Eldoret);

ii. Searching for innovative services on ICT or major improvements to be implemented internally or provided on the external market;

iii. Developing and planning new ICT plans and projects.

2.2 Systems Administration unit

The unit shall be headed by the System Administrator, and it shall be responsible for all activities dealing with feasibility, system analysis, logical design, procurement, implementation and maintenance of administrative information systems. The unit will also be responsible for end-user support in terms of maintenance and development of application programs and databases. The major operational tasks are:

i. System analysis and design

ii. Programming and testing of in-house developed systems

iii. Acquisition of new standard packages

iv. Implementing application software and databases

v. Maintenance, operation system and application software

vi. Establish technical and user oriented documentation of application software

vii. End user software support

viii. Establish and maintain structured system design methods and techniques and System development environment

ix. Systems set-up and configuration

x. Systems security.

In case of centralization of application system development, additional project organization should enable participation of user groups and streamlined acceptance processes. Each information system project may be organized as follows: Project leader, representative of user group, system analysts, programmers and other specialists, such as software engineers etc.

3.0 Network guidelines

3.1 Introduction to University ICT network

The University of Eldoret has developed this ICT policy on network to ensure that ICT services are always available to all authorized users in a more cost-effective way.

This policy deals with the development, expansion and implementation of Data Communication Networks at all levels including common networks, shared networks and individual level networks services.

The common University network includes WIFI, LAN networks and connections between geographically positioned areas (buildings, campuses) and connections to the Internet backbone;

User-level services include emails, Internet access, Internet and Intranet Services.

The shared network services are those networks that make up the combined data Transfer for all ICT services and/or systems. Shared networks may also include off-site data storage, processing and the general operations of cloud computing, Wiring, Hubs, switches, routers, servers, workstations among others, as well as communication protocols (TCP/IP) which are required for the operation of various information systems.

3.2 Objectives of network guidelines

The general objectives of the Network guidelines are:

i) To develop appropriate measures to protect the University's network against unauthorized access;

ii) To highlight the need for network access control;

iii) To establish reliable, efficient and suitable ICT network that guarantees sharing of data, information and other services or resources without compromising the security of the University's electronic resources.

3.3 Networking of buildings within the University.

All new or refurbished buildings within the University shall be connected to the University network as per this policy. Such connections will be done in consultation with the architect of the building or clerk of works. The contractor of new or refurbished buildings shall ensure that all structural requirements for internet connection such as trunking and power cabling and wiring are in place.

3.4 University Back bone

The University network shall consist of a "Backbone" system, and gateway connections to all buildings as well as LANs, and inter-campus connections. These shall be connected to the main computer server via the University's server rooms. The backbone shall consist of a buried fiber-optic cable and where this is unavailable microwave systems links may also be used.

3.5 University Local Area Networks (LANs)

University LANs shall consist of a fiber optic backbone with gateways connecting various buildings within the University and its campuses. The ICT staff member in charge of ICT resources at the main University and in each campus shall be responsible for Network connectivity.

The ICT Director shall make alternative arrangements for those cases where there may be challenges of connecting a particular building in a given campus to the University backbone.

Inter-campuses shall be connected to the University backbone using suitable connections either through radio link or fiber optic cable.

3.6 Private networks

Schools, Departments, offices or sections may not set up their own networks independent of the University Network Backbone. However, if private networks or any other network or extension is authorized, it must not interfere with the University network, and it must abide by the University policies and standards for installation of networks. The ICT Directorate, must be consulted before and during the set up of such networks.

3.7 Computer laboratories, cabinets and ICT network equipment

All computer laboratories shall be manned by competent staff from the ICT Directorate or suitably qualified ICT technicians from respective schools or departments. However for those cases where Schools, Departments or sections establish their own computer labs, these shall be under the responsibility of the said School, Department or section, but they must comply with these policies. Access to University electronic resources to the said labs shall be the responsibility of ICT Directorate.

The ICT Directorate shall own all key network active devices including routers, switches, gateways, bridges, and any other related equipment together with their enclosures. The ICT Directorate shall be responsible for:

(a) Provision of adequate working area with suitable environmental control and sufficient power backups (generators and UPSs).

(b) Regular upgrading and maintenance of all ICT equipment and networks.

(c) Offering advice regarding pricing of ICT network equipments, services and facilities as well as participating in all network repairs, upgrades and maintenance by external contractors.

3.8 Modification of ICT Networks

All modifications to the University network shall only be carried out by staff from the ICT Directorate after written approval has been given by the Director of ICT. Where modifications are outsourced to an external contractor, the relevant ICT staff shall be involved in the modifications.

The Estates Department in consultation with the Director of ICT shall carry out all installations and changes of electrical power cabling in facilities housing ICT equipment.

Installation of any ICT or communication related equipment within the University network shall only be done after approval has been sought and granted by the Director of ICT. The user School/Department shall consult the director of ICT on the specifications of such equipment.

Any other staff wishing to install or maintain a network equipment must always seek permission from the Director of ICT.

3.9 Unauthorized Modifications of University Networks

Any modifications on the Network or any change to the topology of the University or any Modification of the network other than the addition of End-Host Devices is not authorized. Such changes include, but are not limited to the addition, reconfiguration or removal of:

i. Routers;

ii. HUBS;

iii. Network Switches;

iv. Any network hardware device with more than 1 active network connection.

Other examples of some unauthorized modifications of the network include:

(i) Connection of unregistered devices;

(ii) Disconnection of computers from the University network;

(iii) Connection of Hubs, port splitters or switches among others.

Further, any network modification performed without the authorization of the ICT Directorate or by an unauthorized person is not allowed.

If an unauthorized modification is detected, this shall be investigated and connection to the specific network port may be terminated.

If external Contractors are to do ICT network services within the University, they must seek prior approval from the Director of ICT. Once this is granted, they shall only work in the approved areas, and for those working in sensitive areas such as server rooms, the relevant ICT staff shall accompany them.

3.10 Equipment connected to the University network

Each user Department, School or section must notify the ICT Director of any new or added equipment that is connected to the University network, as this may affect the overall performance of the network.

4.0 Guidelines on Access to ICT Resources

4.1 Introduction

The guidelines on access of ICT resources shall ensure that only authorized users access such resources. These guidelines shall be implemented by ICT staffs that have authority to do so by virtue of their job description, and they shall also be in charge of maintenance and management of data or an ICT Service.

Administrators shall be bona-fide members of the University or certified third party support personnel with suitable approvals.

If a member of staff of the University is no longer employed, is suspended from employment, changes their responsibility, or terminates their contract, any administration rights, access or any rights which they enjoyed shall be withdrawn immediately.

4.2 Access to University's ICT resources

Authorized Users of University’s ICT electronic resources (Facilities, Infrastructure and Services) include:

(i) An employee of the University;

(ii) A member of the University Council;

(iii) A bona-fide student of the University;

In addition, any other person can request the ICT Director to become an Authorized User if he/she is:

(i) A member of a collaborative research;

(ii) An associate member, a visiting lecturer or student.

4.3 Administrator Access Requirements

Only relevant ICT staff shall have the administrator authority of ICT electronic Resources (Facilities, Infrastructure and Services) within the University.

4.4 Administrator Account Security

All Administrator Accounts details must always be kept safely as part of the ICT Security of the University of Eldoret.

4.5 Separation of Duties regarding ICT resources access rights

Administrators of ICT electronic Resources (Facilities, Infrastructure and Services) shall be issued with Administrator rights that are equivalent to their jobs.

Clear separation of responsibilities and duties shall be implemented to ensure that nobody bypasses normal auditing procedures.

The Systems Administrators shall have separate functions from other members of staff who are controlling systems storing confidential or financial information, or any system considered to be of corporate nature.

4.6 Generic Accounts

Access of ICT resources using generic (shared, guest, anonymous etc) accounts is highly discouraged. If exceptions are granted to access ICT resources using such accounts, then a clear mechanism of identifying the user of the account must be in established.

Generic accounts must never be used to access systems storing critical or confidential University data, and in case they have to be used, they shall have the minimum rights and privileges.

Use of Generic access to information that is stored in databases can only be allowed for non-interactive processes (i.e tasks not started by a user, nor does the user receive the information) such as scheduled tasks that run automatically or those that are initiated by a series of events such as automatic downloads and other processes for data transfer and updates of anti-viruses.

4.7 Privacy

Electronic information concerned with the use of the University of Eldoret ICT resources shall be collected and may be referred to, in order to ensure full compliance with University Procedures, Guidelines and Policies; and also relevant laws. This shall be done in case a reported or detected misuse of ICT resources or breach of the ICT policy needs to be investigated.

Such information may be given to law enforcement agencies to investigate further any such reported or suspected illegal activity, as per University of Eldoret Privacy Policy, rules and regulations.

4.8 Breaches

Any breach or violation of these ICT resources access guidelines may lead to disciplinary action against the responsible user, as per the relevant university disciplinary procedures.

Users who find out any violation of this Policy are required to report it the relevant ICT staff or any other relevant staff within the University immediately.

In order to prevent unauthorized access to networked services, the University shall implement access control to both internal and external networked services.

Privately owned Devices may be connected to the University ICT Infrastructure only through connection Gateways.

4.9 Connection to Gateways

All privately owned devices connected to UoE gateways must abide by all University policies, procedures, rules and regulations as well as Kenyan laws. It shall be the responsibility of the respective owners to manage of all Privately Owned Devices connected to the University Gateways, and the University shall not be held responsible for managing and/or maintaining such Devices.

4.10 Connection Restrictions

Privately owned Devices shall not be permitted to access Databases or financial systems except in the event that such databases or systems allow a self-service interface for the User.

4.11 Unauthorized Access Attempts

For controlling access to ICT resources, all unauthorized access attempts must be logged. All Audit Trail/System Access Logs shall be reviewed from time to time, and the reports generated inspected by the System Administrator for necessary action to be taken. Such reports of unauthorized access attempts shall be retained by the system administrator who shall produce them whenever needed.

4.12 Internet Protocol (IP) addresses

A distinct IP address shall be assigned to every equipment connected to the University networks.

ICT staff in charge of Networks shall plan and allocate groups of IP addresses to different network segments and to notify the concerned system administrators who shall update their IP addresses register accordingly. In updating the IP addresses register, the responsible ICT staff shall remove any IP addresses that are inactive after three months. The ICT Directorate shall also establish a DHCP server that shall issue IP addresses automatically to devices connected to the University network.

4.13 Connection Disclaimers

The University of Eldoret shall not be accountable for any damage or loss to privately owned Devices.

The ICT Director shall consider requests for connection of privately owned Device to the University of Eldoret network, and he/she shall have the right to reject or revoke any connection request.

In case a violation of this Policy or any other Policy or Procedure of the University of Eldoret is committed or detected, ICT staff shall have the right to disconnect privately owned Devices from University of Eldoret Gateways and network.

5.0 Guidelines on Computer Server Security

5.1 Introduction

The University of Eldoret shall provide computer servers for critical operations such as centralized data, information systems (e.g. student details and confidential financial information), as well as storing large data. Such servers shall be adequately secured both physically and logically so as to prevent unauthorized access.

5.2 Computer Server Ownership and Responsibilities

It shall be the responsibility of the ICT Directorate to manage and monitor configuration compliance of all centralized servers and to administer any exception policies through the respective system administrators. The ICT Directorate shall review and approve any server that is executing critical University processes, as well keeping a register of all details of the servers such as their roles, their physical location, the software and hardware versions that they are using and also details of the System administrator incharge of it.

5.3 Computer server configuration guidelines and server room specifications

General configuration guidelines of all Operating Systems installed in University servers shall be issued by the ICT Directorate. File transfer services e.g FTP or telnet that are not being used shall be disabled to protect the servers, and any access to the servers/services shall be logged. Use of Super-user accounts such as “root” is highly discouraged, and all servers must be installed with updated antivirus software. Logical access to all servers should be through secure channel connections with encryptions like SSH. Servers shall be housed in server rooms that are environmentally controlled and with proper floors, stable power supply supported by generators, UPSs, surge protectors and sufficient lighting protection.

5.4 Control of access to the server room

Access to all server rooms shall be controlled to guarantee their security. Only the system Administrator in charge of a specific system shall be permitted to assign passwords for accessing the respective systems. The system administrator shall also be responsible for the integrity of the system and data, as well as developing end-user access rights. The ICT Directorate shall maintain a register of all passwords of essential network equipments and servers. All system audit logs shall be activated in order to facilitate recording of all log-ins and system failures and also to monitor changes that may be have been effected to the systems.

Every access to server rooms shall be monitored, and this shall only be permitted to authorized staff. Other staff working in the server rooms shall only do so through supervision by ICT staff after prior notification and approval.

6.0 Information Security Guidelines

6.1 Introduction

These guidelines govern the security of use of the University's ICT network. In particular, users will only have access to electronic resources and services which they have been specifically permitted to use.

As such, appropriate authentication methods shall be set up to control access for remote users, by assigning each equipment in the university a unique Identification.

Both physical and logical controls shall be put in place to all ports, while segmentation of groups of information users, services and information systems shall be established on university Networks in order to guarantee efficient and secure management.

The ability of all users to access and connect to the University network shall be controlled, especially for shared networks, and those located in different areas within the University and its campuses. This shall be effected in line with various University business systems, with suitable routing controls being established to ensure that computer connections and flow of data does not breach the network access guidelines.

6.2 Information Security Responsibilities

6.2.1 ICT Director

The ICT Director shall be responsible for:

(i) Ensuring oversight security of all ICT facilities, equipment and other resources within the University;

(ii) Advising the University Management on specialist Information Security;

(iii) Reviewing any security incidents reports and any malfunction or threats;

(iv) Acting appropriately on the received security reports and breaches or violations, or misuse of ICT resources as provided for in various sections of this policy document and also implementing disciplinary measures as appropriate;

(v) Ensuring that adequate security is enforced to all University's ICT equipment and resources;

(vi) Representing the University on law enforcement agencies in matters concerning ICT security.

6.2.2 Deputy ICT Directors

The Deputy ICT Directors shall assist the Director in their respective areas of responsibilities by,

(i) Receiving reports of the University's information systems regarding threats, security incidences and other security related activities that may have an effect on the overall operation of the University's information systems;

(ii) Acting on all received security violation reports within their areas of operation;

(iii) Providing and ensuring ICT security in sections under their control;

(iv) Advising the ICT Director and other University officials on specialist information security;

(v) Guaranteeing sufficient security measures of the ICT resources within their respective areas of operation, developing suitable security standards, and ensuring that responsibilities are assigned and implemented;

(vi) Representing the University on external law enforcement agencies if delegated by the ICT Director, on matters relating to ICT security; and also other ICT security issues as delegated by the ICT Director.

6.2.3 System Administrator

Among other responsibilities, the System administrator shall manage all information security procedures, standards, and controls within the University, in order to minimize any damage, misuse, or loss of ICT resources. He/she shall be specifically responsible for:

(i) Developing and maintaining suitable standards and procedures for accessing ICT resources within the University;

(ii) Selecting, implementing and administering controls and procedures to manage information security risks;

(iii) Giving timely reports on security breaches/violations to the ICT Director and other officers of the University;

(iv) Ensuring that only authorized users access the University's ICT resources and that security of data is always guaranteed, ensuring access and security of data and other application as per the needs of the various system owners;

(v) Liaising with external security agencies if delegated by the ICT Director;

(vi) Documentation and keeping suitable procedures of operation of data integrity, recovery and authentication;

(vii) Providing proper operational controls for data protection;

(viii) Modifying access rights to ICT resources whenever a user is no longer authorized to access University ICT resources or when their job specifications changes;

(ix) Notifying users of their responsibilities with regard to the use of ICT resources and the measures to be taken in case of misuse;

(x) Stopping any unauthorized access to ICT resources, keeping a record of all audit, log-in and other access reports;

(xi) Carrying out every day information security administration process;

(xii) Acting on any reported ICT security breaches as delegated by the ICT Director and ensuring that these are not repeated; and

(xiii) Developing and testing of disaster recovery measures.

6.2.4 System Owners

System Owners shall only be responsible for administrative systems that are directly and centrally controlled, and they shall make decisions on the operations, developments, maintenance and access to the stored data and other applications related to the business operation under their areas of operation. They shall also be responsible for:

(i) Determining suitable security levels, e.g. those involving data transmission;

(ii) Developing processes for users who need information access and reviewing the use of electronic information;

(iii) Taking into consideration request for system access and permitting them as required in consultation with the System Administrator;

(iv) Establishing appropriate measures to ensure data integrity when being accessed;

(v)Establishing suitable data archiving criteria, in conformity to data storage requirements as well as being aware of the relevant legislation and University policies;

(vi) Developing and testing regularly business continuity processes and plans under their control.

System owners shall be required to always update and maintain their respective databases periodically (for example Staff records under Human Resource Information System [HURIS] shall be updated and maintained by Human Resource Department) with the assistance of the system administrator.

6.2.5 Dean of School/Director of a Directorate

A Dean of a School or Director of a Directorate shall be responsible for ensuring that the ICT security policy is implemented within their Schools or Directorates. Whereas these duties may be delegated, it is the Dean's/Director's or equivalent responsibilities to:

(i) Authorize and Approve appropriate data access;

(ii) Consider all security breaches reported against staff and students under their Schools/Directorates and to take necessary action;

(iii) Ensure that staff and students in their School/Directorates are aware of the information security guidelines, responsibilities and other related processes;

(iv) Inform relevant University departments whenever an employee leaves employment or when their contract agreements changes so that appropriate action regarding access of electronic resources can be effected.

6.3 University's Information Internal Audit

The ICT Directorate shall be responsible for assessing the suitability of security measures within the University's ICT infrastructure and information systems.

The ICT Directorate shall also review the compliance with information security procedures and policies when scheduled regular operational audits are done on the University's information systems.

6.4 Responsibilities of Users of Electronic Information

Users of the University's Information & Communication Technology (ICT) Resources are responsible for:

(i) Ensuring the security of their computers by locking them or logging out or off whenever they are not being used and also keeping their passwords safe and secure and never to share them with other users;

(ii) Ensuring the safety of data in their working area and any other systems which they may have access to, reporting misuse and security incidents immediately they become aware of them to the ICT Help Desk and also through the email shown on the University website.

Users of the University's ICT resources for research, teaching, learning, professional or personal advancement are further advised that they must do so in a manner that advances the University's mission of achieving its goals and objectives. This use must also support the operations of the University and promote its good name. Whereas staff and students may use the University's ICT resources for personal gain, such use may only be kept at a minimum.

6.5 Compliance

Violation of the information security is a severe offense and the University shall investigate such violations and take disciplinary action against any user who breaches of the ICT guidelines on information security.

Any account that is suspected of having been misused or one that is under investigation may be closed temporarily or permanently until the abuse or misuse is fully resolved. Similarly, any equipment that is misused may be impounded or any material that breaches these information security guidelines may be taken away from the University website.

6.6 Creating Awareness

Due to the sensitivity of information security such as privacy, confidentiality and system access, it is essential to induct newly employed staff on information security and also to give the same information to staff already in employment. The ICT policy shall be posted on the University website for much wider access by all authorized users.

Once employed, every employee should be made aware that they should not reveal any information that they may access in the course of their duties. They must also be made aware that they should never try to access information that is not needed for their daily duties.

Newly registered and also continuing students must also be made aware of their information security responsibilities.

7.0 Guidelines on E-learning

7.1 Introduction

These guidelines are meant to outline the usage of e-learning within University of Eldoret, and also to ensure that authorised user access e-learning content in an efficient and ethical way. The student numbers within the University has continued to increase and this trend is expected to continue. Use of electronic technology may therefore assist in assessment of students.

Through e-learning, a lot of content is now available to students. In order to maintain quality it is therefore expected that student projects, theses and assignments shall be submitted in both soft and hard copy to enable testing with university approved anti-plagiarism software.

7.2 Role of e-learning

E-learning provides a strategy to respond to three major challenges: Cost, Quality,
and Demographics.

7.3 E-Learning Goals/Objectives

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

1. To improve the quality of graduates, by utilizing modern instructional materials and methods, including increased use of ICT in teaching and research.

2. To provide greater access to University education, by developing capacity for increased enrolment through non-conventional approaches in teaching and learning i.e. Distance education and virtual university.

7.4 Management of E-learning

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

The University shall use a platform that enable students and lectures to access e-learning everywhere in the world. As such, the University recognizes Learning Management system (LMS) as key to delivering content through e-learning. The LMS is expected to be user friendly, can support third-party additions, can support multi-user facility with good security features. It should also facilitate easy access and support updates of content among other essential features.

7.5 Open and Distant Learning (ODeL) Unit.

An Open and Distant Learning Unit shall be established within the Directorate of ICT and it shall be mandated to:-

(a) Work as an e-learning service provider.

(b) Coordinate e-learning activities.

(c) Vet proposals on e-learning.

(d) Monitor and evaluate e-learning at University of Eldoret.

(e) Promote e-learning through awareness seminars, workshops etc.

The proposed unit should be lean, and it should have all the core functions of e-learning management. Its staffing shall be as per the ICT strategic plan.

8.0 Guidelines on Electronic mails (Emails)

8.1 Introduction

For purposes of storing and accessing Electronic mails, the University shall dedicate computer servers which are managed by the ICT directorate.

8.2 Objectives

1. To inform users of their roles and responsibilities when using University's Emails.
2. To determine the resources required for the Electronic Mails.

8.3 Activation of email/account

Whenever a staff member, student or visitor becomes an authorized user of the University's electronic resources their email accounts shall be activated.

8.4 Account Creation

If a current student, through admission/registration or a current staff member, through the advice of Human Resources Department becomes an authorized user, their email accounts shall be created and activated.

Any user of the University's electronic mails shall need a user name and password, issued only by the ICT staff.

All email accounts shall only become active after the user fills an application form to request for use of University's email resources.

8.5 De-activation of Electronic Messages (email) Accounts

An account shall be deactivated when a staff member retires, resigns, terminates his/her employment, the use is considered improper or when the Dean/Director or the Human Resources Department/Registrar (Administration) considers such a staff member as being absent without leave after their employment is terminated due to lack of a formal notification of the University, and notifies the ICT Director of such decision.

A student's account shall be deactivated after he/she has graduated, has not registered for their programme of study, has been expelled from the University, use of the account is deemed improper, has withdrawn or has terminated their studies, has discontinued their studies without formally notifying the University and has not registered in another study programme, and after the Registrar (Academic) has notified ICT Director of this in writing.

Email accounts for visiting lecturers shall be deactivated when they terminate their contract, consultancies or visiting arrangements with the University, or if the research project ends.

8.6 Re-activation of Email Accounts

Newly admitted students and newly employed staff shall have their accounts activated as well as those staff whose accounts had been de-activated or suspended following successful appeals.

8.7 User's Obligations to using University's email services

It is the responsibility of all users to maintain network traffic low by compressing large messages and attachments before sending the emails.

8.8 Unacceptable Activities on use of emails

While users may not be stopped from getting offensive emails, they shall still be required to use email services professionally and in an ethical way by avoiding the following:

(i) Sending emails unnecessarily or sending or distributing junk emails, SPAM or chain letters;

(ii) Sending offensive, defamatory or abusive emails or harassing others;

(iii) Causing harm to minors through emails;

(iv) Sending illegal electronic messages or those that breach other University policies, procedures, rules and regulations;

(v) Making available any information that they do not have rights to;

(vi) Sending chain letters of emails, resending same emails over and over again, impeding others from using emails, and sending of uncalled for emails;

(vii) Impersonating the University or pretending to make statements on behalf of the University;

(viii) Distributing unidentified Emails, or forged emails or pretending that they originate from another user;

(ix) Using emails unreasonably or interfering with other users of emails;

(x) Sharing accounts, usernames and passwords;

(xi) Unauthorized Security scanning of any port;

(xii) Unauthorized interception of data, blocking others or interfering with access of networks;

(xiii) Bypassing authentication of users or security of a given computer, account, and network;

(xiv) Using computer scripts, codes, commands or programs to disable or interrupt other users' computers;

(xv) Unauthorized changing, accessing, copying or deleting of emails of other users;

(xvi) Unauthorized commercial activities or deriving personal profit using University's email resources;

(xvii) Deliberate or unintentional introduction, propagation, creation or distribution of computer viruses.

8.9 Email Account Privileges

Account privileges shall be assigned in such a way that every user has access rights which are only sufficient for their duties at the University of Eldoret.

If the duties of a User within the University changes or are terminated, their rights of access shall be altered to conform with the requirements of their current status.

8.10 Email Account Auditing

Email accounts shall be audited from time to time, in order to remove inactive ones, establish the unauthorized accounts or those accounts that have never been used; or to issue new email allocations or remove some privileges as per this policy.

8.11 Email Account Security

Account security must be maintained according to the specifications/procedures of Username and Password. If emails shall contain attachments that are considered dangerous to the security of the system, or emails that lie within the specifications of article 9.0.9, these may be blocked.

8.12 Activities for profit or advertisements

Unauthorized commercial activities or those of personal gains are not allowed when using University email services. Approval for any advertising or sponsorship of any activity must first be sought and granted from the relevant University office.

8.13 Message Storage

Electronic mails shall be stored both on-line and off-line for agreed periods as per regulations and other policies, to allow for regular and routine backup operations. Emails may also be archived for recovery purposes.

8.14 Domain name services

All activities involving Domain Host Control Protocols (DHCP) and Domain Name Services (DNS) within the University shall be controlled, managed and monitored by the ICT staff.

8.15 Support and maintenance procedures of emails

8.15.1 System Accountability

Although the ICT Directorate shall be in charge of the physical and logical security of electronic messaging services, the University shall be not be held liable for any loss of electronic messages. Also, whereas, ICT staff may inadvertently see contents of emails during their duties, they shall not do so intentionally or disclose the contents to anyone else or use the information, unless provided for elsewhere in this policy. The systems administrators are however exempted from this, since they may need to examine the contents of messages as part of their duties. Owing to the very nature of electronic messaging systems, the University is not able to guarantee the absolute confidentiality of information. The University also takes no responsibility for emails transmitted through its electronic resources systems.

The University respects the privacy of users, and it has no desire of routinely inspecting or monitoring emails. Nonetheless, it may be necessary to view contents of stored emails from time to time, as part of the requirements of the Freedom of Information, with a view to redirecting emails which cannot be delivered, or to view contents as part of the legal provisions, or for filtering emails that could lead to system failure, or corrupt messages or messages containing viruses. In all cases, the concerned user shall be notified so as to give consent to examine or monitor emails. System logs may contain the sender and originator addresses of both incoming and outgoing electronic emails and all users must be cognizant of this.

8.15.2 Inspection of Electronic Messages (emails) without Consent

If emails have to be monitored, examined or their contents disclosed without consent, the following conditions shall apply:

(i)This measure conforms to law and it's also required by law;
(ii) Violation of University policy or relevant laws has occurred; or
(iii) To fulfill time-dependent operations that are critical to certain transactions.

If there is need to access a user's emails as per any of the above conditions, then a request for authorization shall be sought, and in cases of emergencies this may not apply as explained in sections 8.15.3 and 8.16 respectively.

8.15.3 Request for Authorization

Except in cases of emergency, authorization must always be sought and granted in advance and in writing by the relevant authority according to the law or policy for certain actions to be taken. If a certain authority is not clearly specified, advice of the ICT Director must always be sought together with that of the Legal Officer due to changes in interpretations of laws dealing with privacy of emails. The affected person shall normally be informed as soon as possible of any action taken and the reasons for this action, unless Kenyan Laws or other University policies demand otherwise.

8.16 Emergencies

In cases of emergency, for example when the institution or its members are facing any danger or to keep the integrity of information services or access to emails needs to be controlled to ensure the preservation of evidence, special steps shall be taken. The ICT Director shall in such cases take any necessary, suitable and immediate actions to deal with the emergency, without necessarily having to seek authorization first, although authorization must be requested immediately following the procedures described above. The ICT Director shall be required to restore the situation to that which prevailed before the action was taken or at least close to it, if the action taken is not authorized.

8.17 Email Backups

Emails shall be backed up on a weekly basis so as to restore information if the system fails or if the entire mail system or individual email accounts are corrupted. Users must however be aware that email backups shall not be used for restoring lost or deleted emails.

8.18 Compliance

All users are responsible for reading and complying with these procedures on emails and any associated guidelines, conditions of use, the relevant laws and policies. Any user who logs onto their accounts is bound by the conditions of this procedure and other applicable University policies, rules and regulations governing the use of emails and other ICT facilities and resources within the University.

9.0 Guidelines on Acceptable use of ICT Resources

9.1 Introduction

The university shall provide adequate ICT resources that must be used in an acceptable manner by all users. Any alleged breach of the University of Eldoret's ICT Acceptable use guidelines shall be reported to the ICT Director who shall record and carry out the necessary investigations and take appropriate actions as per this policy.

This policy is further intended to guarantee acceptable use of ICT resources as well as protecting the resources such as information, software and hardware against unacceptable use, and guaranteeing the integrity, use, recovery, validity, security, privacy and availability of the University's ICT infrastructure.

9.2 Objectives

1. To ensure that all staff and students use the ICT resources in an acceptable, responsible and ethical manner.
2. To ensure that all breaches of the ICT policy are attended to and addressed appropriately.

9.3 Risk Management

From time to time, and in order to mitigate on any risks to ICT infrastructure, the University shall conduct risk assessments of its information systems to determine any potential compromising situations and then take remedial security measures to reduce the established risks.

9.4 Access Authorization

All users of electronic resources of University of Eldoret must be authorized to access the University's information systems. In order to ensure acceptable use of University ICT resources, all access shall be controlled and monitored by the ICT Directorate as per the provisions of this policy and any other relevant University policies.

9.5 User Identification/Authorization

All users of information systems within the university shall require a unique user identification (ID) and a password for validating their identity and hence to be able to access the University's ICT resources. Such details must be kept securely, and users are further prohibited from sharing their user IDs since every user shall be responsible for any unacceptable use activities originating from their ID.

The ICT Director may approve the issuance of temporary or generic accounts under some special circumstances that are well justified and controlled, as mentioned elsewhere in this policy.

9.6 Access Rights

Authorized users shall only be given access rights to University's ICT resources that are proportionate with their job entitlements.

9.7 Account Management

System Owners are required to review their schedule of delegated authority periodically, with a view to determining the users that are authorized to access the system and their permitted levels of authorization.

In order to ensure full compliance with this policy, all system access levels shall be reviewed annually and any detected non-compliance addressed immediately. System owners are required to always maintain records of all non-compliance events, until all matters related to them are fully attended to.

9.8 Privileged Users

System Administrators shall have higher access privileges, granting them access to any information that is stored on the University of Eldoret's information systems. While executing their duties, they shall be expected to adhere to their Code of Ethics and must sign at least an annual confidentiality agreement. Any breach of this Code of Ethics may result into disciplinary action according to their employment agreements.

Sometimes Contractors or/and third-party members may be granted access as long as the System Owner is informed and is in agreement to this arrangement and that a full-time University staff is involved. The Contractors and/or third parties must always abide by the access control guidelines whenever accessing the University's ICT resources and that they must have at least a unique user ID to authenticate every user as per article 9.5 of this policy. Any temporary accounts given to the contractors or third parties must have an expiry date that is determined by the date of completion of the contract, or some suitable agreement established with regard to the contractor or third party's access.

9.8 Access to Electronic Resources Operated by Third Parties

All users granted access to information systems and resources that are operated by third parties must ensure full compliance with the relevant Information Security and Acceptable Use policies applicable to such information systems and resources.

9.9 Accessing the Internet and Online Services

Only authorized users shall be able to access the Internet and other online services provided by the University, as per the requirements of the acceptable use of ICT resources, other legal requirements, Kenyan laws and other relevant University procedures and Policies.

9.10 Internet and Online Services Access Restrictions

Any access to internet and online services that is considered to be in violation of the Kenyan laws, university policies and other regulations shall be restricted.

Whenever formal complaints are launched or violation of these policies or rules have been detected or reported, appropriate measures shall be taken to ensure restrictions of usage.

ICT access restrictions shall be put in place on any online services that are considered to be involved in unacceptable activities such as distributing viruses, malware, or solicits personal or financial details.

Such online services or websites that are blocked due to the conditions set above and also elsewhere in this policy shall not be permitted to be used for research, learning, teaching or any other University-related business operations.

9.11 Internet Security

Users are informed that any computer or server that is connected to the internet is exposed to a certain level of security risk arising from unauthorized access or unacceptable use. Thus, adequate security measures need to be put in place to prevent such internet security risks.

9.12 Appeals

Staff and/or students whose access to online or internet resources has been suspended or blocked for reasons mentioned elsewhere in this policy document shall be able to appeal in writing to the ICT Committee/Director and appropriate measures taken.

10.0 University Website

10.1 Purpose

A well designed University website with quality content can give the University of Eldoret greater visibility and an edge in the digital world. The University shall therefore maintain a well designed website for access by all users and the general public.

10.2 Introduction

This policy is meant to ensure that the University's visibility on the world of digital information is greatly enhanced, that all web pages hosted on the University website conform to the set standards and guidelines and that they must be hosted in consultation of the ICT director.

All pages must be located and accessed through the official University Website: http://www.uoeld.ac.ke and they must convey the mission and vision of University of Eldoret. Only the University logo, colours and standard fonts must be used in all web pages to be hosted on the University web site. Sizes of the files to be hosted in the web pages shall be as small as possible to facilitate faster downloads.

Before a web page is hosted on the University website, the Dean of School, Head of Department, Administrative office or Head of Section wishing to host such pages must seek approval from the ICT Director through writing. The Dean of School, Head of Department, Administrative office or Section must also approve the proposed content before it is submitted for hosting and also appoint a content owner. Users are advised adhere to the following procedures before any content is hosted on the University website:

(i) Clearly define the objectives of developing the web page;

(ii) Establish and develop the content of the web page;

(iii) Submit a list of all links to the web page;

(iv) Establish a schedule of developing the web page.

For approval to be granted, the following shall be considered:

(i) The relevant reasons of using the internet for the specific communication;

(ii) Academic worthiness of the web page in relation to the mission and vision of the University;

(iii) The web page is in conformity to the set standard and portray a good image for the University;

(iv) The web page must be unique, not a duplicate of others and it should also be easily incorporated with other web pages.

Upon fulfillment of these requirements, the ICT Director shall allow the hosting of the web page but the final approval shall be granted by the Vice-Chancellor.

The University website shall only host internal resources of information, with suitable links being established to external sources. Any links to the University website as well as filtering of unsuitable web-based or non-web based internet traffic shall be authorized by the ICT Director.

10.3 Managing a Webpage

After a web page is approved and uploaded, the content owner shall:

(i) Keep updating the web page according to the set timelines of publishing;

(ii) Ensure that all necessary approvals for updating the web page are requested and granted;

(iii) Respond to all questions/feedbacks promptly.

All Extranets and intranets developed within the University together with their maintenance schedules must be in conformity with all the approval procedures mentioned above.

10.4 Web page cache provision

The web page cache shall be managed by the ICT Directorate to ensure provision of proper services to the University community.

11.0 Guidelines on Data Backup

11.1 Introduction

This policy gives guidelines on the backing up of data and information within the University. The University shall therefore dedicate suitable computer servers to backup data, both on-site and off-site.

11.2 Data Backup Scheduling and Retention

For business continuity in case of system failure, all data held on production servers shall be backed up to according to set schedules, depending on the nature of the server. Users are expected to back up data that is kept in their computers or workstations, and also backup copies of important documents or files on safe drives or on shared network drives and also on CDs and DVDs. These may be then stored in a suitable environment or in fireproof cabinets.

Data back up shall be done daily and also weekly and preferably on weekends for data from information system servers in order to reduce interruption to business processes. Incremental daily data backups shall also be done every night for continuous backing up and this shall be stored for a minimum of seven days. In backing up, the most recent data shall be kept on-site, and the rest of the data shall be kept outside the University premises. Data shall be backed up every 15 minutes for the on-site server, while for the off-site server, data shall be backed up every night. In order to avoid loss of any transaction, all production servers shall be configured in such a way that all data is replicated in all them.

In addition to these scheduled backups, the ICT Directorate may backup data at other periods as dictated by the circumstances, and/or as advised by the system administrator in charge of the respective servers.

It is upon each user School/Departments/Section/administrative office to establish the data that needs to be backed up, and also the method of storage as advised before.

Each user shall back up and also establish the schedule of backing up data that is stored in other places including servers, desktops, laptops and/or other mobile devices.

11.3 On-site Data Storage

All on-site data storage shall be stored in a safe and environmentally controlled area (data centre/server room), and this shall only be removed for restoring the system, or taking the storage material/media to an off-site storage as per article 11.2. This back up material/media shall only be accessible to ICT staff whose job descriptions permit them to use it.

11.3 Full System Recovery

In case of system recovery, production servers shall be restored first while other restorations shall be prioritized after the users have notified the ICT technical staff of the problem via the ICT help desk or either physically or through email as provided in the University website. In order to minimize cases of system failure occasioned by power interruptions, redundant cabling, interruptible power supplies and power generators shall be connected to all servers executing and storing important University data such as information that is stored and accessed centrally.

It is recommended that backed up data should be accessible for full system recovery within less than 12 to 24 hours all the year round. Also, backed up data must be tested periodically (preferably after quarter of a year) to guarantee full system recovery in case of a real system failure and that all restoration procedures must be documented and kept safely. These procedures must be tested at least every six months.

Departments/Schools must also ensure that they document and keep all backup and restoration procedures for all their servers, computers and hosted applications.

11.4 Computer Servers being hosted outside the University premises

Whereas the University may store data in servers hosted outside its premises, users ought to be aware that the University may not have the capacity to protect such computer servers directly together with the other applications through its regular back up procedures. However, the University shall ensure that data stored outside the University premises is kept safe against any disaster. It is the responsibility of every user to ensure that any service level agreement that they enter into hosting data outside the University is adequate for their need, and that it is consistent with this policy with regard to safety, recovery and documentation.

11.5 Requirements for Off-Site data Storage

Any off-site storage location must have sufficient protection against fire, has enough environmental controls, and is well protected against theft and that it satisfies any other necessary requirements for server hosting. Users must enter into a formal Service Level Agreement (SLA) with the provider of the off-site storage facilities, and that they must make site visits to the facility at least yearly.

11.6 Data Retention

Determination of data retention period shall be the responsibility of the owners of University data, who must also specify the responsible parties, the retention period, the legal requirements and also their sources. The responsible system Administrators shall then ensure that any requirements are complied with.

11.7 Business Continuity and Disaster Recovery

The University shall develop suitable disaster recovery plans and policies which shall be tested regularly for those servers executing key University processes so as to ensure Business Continuity if any system fails. Adequate Risk Management structures shall also be established and tested periodically, with the importance of the systems to the operations of the University business dictating the strategy to be employed for full system recovery after a disaster in a timely manner.

11.8 Physical Security of server rooms and computer laboratories.

Access to secure areas, including server rooms, computer rooms, laboratories, rooms hosting network equipment and any related facilities, is only permitted to authorized University staff and students. Server rooms shall be locked, and all wiring closets and data cabinets shall also be locked to guarantee their safety, and also to protect them against any damage. This shall also prevent unauthorized connection attempts to data outlets or unauthorized swapping of the cables from different ports that may slow down the network. Any repairs to server rooms or other rooms hosting critical University ICT equipment shall only be done by the Estates Department staff in consultation with ICT Directorate. All ICT equipment shall be protected against power surges by installing anti-surge protectors and also ensuring that lightning arrestors are installed in all buildings within the University.

12.0 Guidelines on Information Classification and Data Usage

12.1 Introduction

During its day-to-day operations, the University shall generate, or use different types of Data. This data may be classified as Public, Proprietary and Restricted. Every type of data or information shall have an owner who shall authenticate and authorize the processes corresponding to the respective data categories.

Out of these categories of information, any data classified as public can be distributed to the general public, while proprietary data is for internal University use and is not meant for external distribution. Restricted data whose sensitivity levels lies between moderate and highly sensitive, is only accessible to staff who need it to carry out their duties, and it also protected by Kenyan laws.

Every user must ensure that they are aware of their legal and corporate responsibilities in respect to unacceptable use, sharing or releasing data to other parties. It is the responsibility of any user accessing proprietary or restricted data/information to seek appropriate authorization. In doing so, they must also ensure that they or their Schools/Departments/Directorates have established information security measures, in order to guarantee confidentiality and wholeness of that data as per the relevant University policies and guidelines.

12.2 Objectives

1. To ensure proper handling of information and data.
2. To ensure that users are aware of their responsibilities with regard to use of information and data.

12.3 Care and Handling of External Data/Information

Sources of external information include that which is collected, purchased, and/or given by the owner. Often times, such information may be copyrighted or the confidentiality agreements demand certain conditions of use. While using any external Information, the University shall respect any agreements associated with the use of the information.

12.4 Care and Handling of Internal Data/Information

Internal Information is any information that is collected and managed by the University. Such information belongs to University of Eldoret and all University policies, procedures and guidelines shall be adhered to while handling it.

12.5 Misuse of Data/Information

Any use of data either unintentionally or deliberately which breaches University policies or breaks the Kenyan laws shall be classified as data misuse. This includes but not limited to:

(i) Obtaining or accessing data that is not within one's job specifications;

(ii) Accessing or downloading centrally held data to unauthorized equipment, databases or devices;

(iii) Unauthorized personal profiting from University data;

(iv) Issuing or accessing data without following the correct channels and approved procedures;

(v) Using information or data inaccurately or disobeying any established and/or approved procedures on data usage.

13.0 Guidelines on use of ICT Services, Infrastructure and Facilities

13.1 Introduction

The University shall avail ICT services and facilities for use by all authorized users. These guidelines are meant to streamline the use of all ICT services, infrastructure and facilities within the University.

13.2 Asset Security Management

All key information systems within the University shall have a member of staff who shall be responsible for implementing and managing these guidelines with regard to such assets.

13.3 Security of Software

It is expected that all software being used within the University is properly licensed. Such software must be properly documented, tested and archived with all patches as well as new versions or upgrades before being used.

It is also expected that all operational software is kept at the current versions or be maintained at the latest levels that are supported by the suppliers. In some special cases, a version of software that is not necessarily current may be may retained. It is further recommended that all applications developed by, or within the University or software that is purchased from external suppliers must be developed with appropriate security controls.

Users are required to report any misuse of ICT resources to the ICT Director as well as other security incidences such as port-scan attacks or unauthorized access to some special high level accounts.

13.4 Computers/Workstation Security

Computers/workstations connected to the University network shall be configured periodically, so as to update the installed applications and operating systems. Only licensed anti-virus software shall be installed on university computers and workstations, and the automatic anti-virus update shall be activated during configuration to ensure that the computers/workstations are protected against viruses and any other malicious scripts or computer codes.

Unless authorized, users shall not have administrative rights to their computers or workstations. Further, only ICT technical staff shall assist with all installations of software and changes to configuration on all university computers/workstations.

13.5 Mobile Device Security

It is the responsibility of all users of mobile devices who carry out University business on them to protect them and any information stored in them against any loss or disclosure of the information to other parties. All mobile devices must be fitted with passwords/PINs with time-outs to enable the devices to lock after some time to minimize chances of unauthorized access in case they are left unattended. Although the University may permit mobile devices to access online resources via wireless network, their access to restricted or secure data shall be limited. Such devices shall also have encryption to prevent unauthorized access to data stored in them. Downloading of restricted university data shall not be permitted on mobile devices, unless authorization is granted by the respective owner of the data.

13.6 Monitoring of ICT Facilities, Services and Infrastructure

ICT staff shall periodically monitor and collect data on usage of all ICT Facilities, Services and Infrastructure within the University for purposes of establishing compliance with University policies, rules, regulations and any relevant Kenyan laws.

13.7 Privacy

If there is a reported misuse of University of Eldoret ICT resources, any information collected as per article 13.6 may be accessed to investigate such allegations. The information or report on unlawful activities may be handed over to the Kenya police service to investigate such acts, as per the University's Privacy Policy and guidelines or Kenyan laws.

14.0 Guidelines on Security incident notification and reporting

14.1 Introduction

The University takes cognizant of the fact that there shall be security incidences relating to the use of ICT services, facilities and infrastructure. This policy gives guidelines on the procedures of reporting any security incident concerning the use of University's ICT resources.

14.2 Definition of a Security Incident

Any act or event that contravenes the provisions of this Policy document shall constitute a security incident, and this may also include violation of the Kenyan law.

In particular, in order to ensure sufficient security measures, all premises where University servers are residing shall be fitted with both visual and/or audio alarms and such premises shall only be accessible to staff members with the necessary rights.

14.3 Notification of a Security Incident

Users who become aware of a security incident shall take the following steps as soon as possible:

i) Notify the ICT Director using the ICT help desk or email address given on the University website or through some other suitable method. Any account that is believed or found to have been misused shall be de-activated immediately and without any prior notice;

ii) The Kenya Police service shall be notified by the ICT Director if the security incident concerns a violation of Kenyan or International law;

iii) If the security incident involves a directorate/department/section within the University, it shall be communicated immediately through the Dean of the School, Director of a Directorate or the Head of Department or Section;

iv) If the security incident concerns an organization or somebody outside the University, the Kenya Police service shall be informed immediately.

v) In case an organization/institution or somebody outside the university is a potential victim of a security incident, the organization/institution or individual shall be informed as soon as possible.

14.4 Reporting and Investigation of a Security Incident

The staff member authorized to conduct technical investigations on a reported security incident shall do so by adhering strictly to the laid down procedures. He/she shall make a report concerning the incident for the ICT Director, who shall consider and approve the report, and then forwarded to the relevant Dean of School/Director of a directorate/Registrar or Head of Department/Section with the following details:

i). Nature of the security incident;

ii). The nature of the persons concerned in the security incident, i.e. whether they are members of staff, students, external clients, system etc;

iii). The computer used in the security incident;

iv). The security incident details;

v). Any real or perceived impacts of the security incident;

vi). Suggest steps to be taken to avoid a repeat of the security incident;

The concerned Dean of the School, Director, Head of Department/Section or Registrar shall implement the recommendations of the report. However, if a higher security risk is established, the ICT Director shall assess it following the University's Risk Management procedures and any other relevant disaster Recovery Plans and take the relevant remedial measures to prevent it.

15.0: Guidelines on Telecommunications

15.1 Introduction

The University shall give staff members phones and/or voice-mail whenever available and as necessary to carry out University business. This policy outlines the guidelines on the use of telecommunications devices within the University.

15.2 Monitoring Phone Usage

Departments and Schools shall monitor their monthly usage of the phones and/or phone cards, and verify the invoices received. Personal use of these phones is highly discouraged.

Schools/Directorates/Department/sections are advised to call from Mobile phones only when there is no suitable alternative so as to reduce the call charges.

16.0 Guidelines on Software Copyright Provisions and installation

16.1 Introduction

The University realizes the need to respect all copyright laws. For this reason, it does not permit any of its ICT resources to be used for activities which may breach any copyright provisions.

Further, these guidelines outline the measures to be taken with regard to installation of software on University owned electronic devices and equipment.

In order to ensure that this policy is adhered to, the ICT Director shall approve and authorize any alterations to the operating environment of all ICT devices and equipment, which includes among others any additional software and/or modifications to the configuration.

16.2 Objectives

1. To inform users of their responsibilities on the use of copyrighted software.
2. To inform users on the requirements for installing software on University owned devices and equipments
3. To ensure that University's ICT equipments and devices are installed with genuine software.

16.3 Guidelines on Software copyright licenses

University of Eldoret shall respect all the existing copyright licenses as well as computer software copyrights which it has signed into. The University shall not allow users to copy or duplicate any software that is licensed nor permit the use of unlicensed software on its ICT facilities, resources or its premises except in a situation where the licensing authority has granted such permission.

16.4 Acquiring Software

Users must justify the need for purchasing any software, and that all software must be clearly documented so that it can be adequately registered, supported and also to ensure upgrades of all software that is acquired. These provisions apply to software that is also obtained through the internet.

16.5 Authorized Software

Authorized software shall meet the following requirements:

(i) Abides by all terms and conditions of the license;

(ii) Must be tested by an ICT staff for abidance with the established security measures and also utilization of ICT resources;

(iii) Must be installed by an ICT staff or in consultation with an ICT staff.

16.6 Unauthorized Software

Unauthorized software is categorized as one that does not fall in the category outline in section 20.1, and further it fulfills the following criteria:

(i) One whose usage violates the terms and conditions of the license;

(ii) It has not been tested nor installed by an ICT staff nor in consultation with the ICT Directorate;

(iii) A software that has not been authorized by the ICT Directorate.

16.7 Unlicensed Software

Unlicensed software includes any software that breaches the existing license agreements and it is prohibited from being used on University of Eldoret's ICT Facilities, until all the requirements of the software licensing have been fulfilled. It shall be a breach of this policy to install any software on University owned devices or equipment that does not satisfy the license agreement terms.

16.8 Installation of Software on UoE equipment.

Only technical staff from the ICT Directorate shall install all software on University's ICT facilities. The ICT Directorate shall also be responsible for storage of the original installation media and the accompanying manuals, and in certain cases by the user depending on the situation.

16.9 Installation of software on University Computers

Computers owned by UoE must always be installed with licensed software as well as anti-virus software. It is strictly prohibited for users to bring their home software to install it on UoE computers unless such an arrangement has been allowed by the ICT Director depending on the licensing agreements.

16.10 Use of ICT Services and Facilities with regard to copyright provisions

Copyrighted materials that are recognized by the University include:

(i) Music

(ii) Movies

(iii) Television programs

(iv) E-publications

(v) E-books

(vi) Electronic journal papers

(vii) Computer software

(viii) Unlicensed data

16.11 Provisions of UoE ICT resources regarding Material that is Copyright Protected.

It shall be prohibited for any user to copy, compress, download, store, redistribute or transfer any copyright protected material on University of Eldoret ICT resources.

Any material that infringes the copyright provisions shall be removed from the University's ICT resources without notice. Access to services or websites outside the University that are suspected of being used as the origin of violating material shall be blocked without notification.

16.12 Responsibilities of UoE Members in Relation to Copyright Protected Material

Users are not allowed to carry out activities on the University's ICT resources that violate the copyrights of the holder. Such activities include storing, obtaining or sharing any copyrighted materials among others, as per article 18.7.

From time to time, UoE ICT users shall buy ICT materials over the internet and such material must not be stored on ICT resources unless it conforms with the existing license agreements. All UoE ICT users are required to adhere to all legislative and other policy provisions on copyrighted materials.

16.13 Use of Copyright Protected Material for Teaching or Research

The University of Eldoret shall hold certain licenses that permit some copyrighted materials to be copied, stored or transferred, for teaching and research purposes. Such materials shall include but not limited to those mentioned in section 18.6, and all users are expected to adhere to the existing license agreement when using these materials.

Information regarding the use of copyrighted material for research and teaching purposes shall be provided by the Librarian and also posted on the University's website (http://www.uoeld.ac.ke).

16.14 Private Use Conditions of copyrighted materials

The Copyright Laws of Kenya allows users with some rights in relation to the Private use of some copyrighted materials which they have purchased. Such rights include modifying the format of some recordings of music or images to enable them to be audible or visible in some devices, provided that the original copy does not violate the copyright agreements. Other conditions of private use included domestic use only, and that the user owns the device onto which the music or image are to be copied.

Users shall not be allowed to copy or store or redistribute electronic materials such as music or videos on University of Eldoret's ICT resources, even if they own the material, if this violates the Private Use conditions of the Copyright Laws of Kenya.

16.15 Notices of Copyright Violation

University of Eldoret shall ensure that all license conditions of copyright materials are not violated, and that the University's ICT resources are not used to infringe on the copyright provisions.

Any material in violation of the copyright agreement shall be withdrawn from the University's network immediately, and the University shall also disconnect any equipment/s used in the alleged violation, until the situation is fully addressed.

Users shall be required to notify the ICT Director of any copyright infringement using the ICT help desk or some other appropriate means as outlined in section 14.0.

17.0 Guidelines on Software Development, Support and Use

17.1 Introduction

Students and staff of the University of Eldoret may develop software either for personal, office and research purposes.

17.2 Objectives

1. To inform software developers of their responsibilities in the development, support and use of softwares.
2. To establish the regulations and guidelines to be followed for any software developed in the University.

17.3 Software Planning, Development and testing

Any software developed within the University shall have an owner or leader whose responsibilities shall include the planning, development, testing and implementation of the software. In its initial stages of development, the software must be tested off-line in consultation with the ICT Directorate, if it is to be used on the University's Network. The developer shall ensure that the software is copyright protected and that it is in conformity with all software copyright laws and that it is developed in line with all University policies. The software applications must also support all necessary user authentications, as well as all appropriate security features.

18.0 Guidelines on Cloud Computing Services

18.1 Purpose

These guidelines outline the use of cloud computing services within University of Eldoret with regard to supporting the sharing, exchanging, processing, storing, and managing of institutional data/information.

18.2 Introduction

Cloud computing has become key to providing ICT resources that the University may not otherwise have the capacity to own, such as hosting students emails. Cloud computing is therefore expected to help the University to take advantage of the available powerful computing resources by accessing various services, applications and infrastructural resources over the internet.

18.3 Getting access to Cloud Computing

Authorized users may access cloud computing facilities over the internet, using either laptops, desktop computers, workstations, smart-phones or even tablets, at very small or no cost depending on the existing service level agreements with the service provider.

However, whereas use or access of cloud computing resources is recommended in certain circumstances, users need to be aware that there are some certain unspecified risks whose level may increase with no prior notice to the end user such as:

(i) Lack of clearly established security steps regarding storage and accessibility of information through cloud computing.

(ii) Loss of cloud computing services abruptly and without notice.

(iii) No guarantee for Users privacy and intellectual contribution when accessing or storing information on cloud computers due to lack of guarantees on security of data.

To mitigate and safeguard the University against these risks, it is recommended that the University enters into suitable service level agreements with the appointed service providers.

19.0 Guidelines on Password Policy

19.1 Introduction

UoE equipments and devices shall be accessed through suitable usernames and passwords. All authorized users are therefore expected to have passwords to enable them access their accounts, and also for user authentication. The initial passwords shall only be issued by ICT system administrators or by other system owners with sufficient powers owing to their job requirements.

19.2 Objectives

The objectives of these guidelines are:

(i) To ensure that users are aware of their responsibilities with regard to use of password.

(ii) To ensure that users know the characteristics of passwords.

(iii) To ensure that users understand the security implications of their passwords.

19.3 Password usage and requirements

The requirement of passwords depends on their level. In particular, Users are advised to change root and system passwords every month, while user passwords are recommended be changed in every three months. Super user passwords must be strong and clearly distinct from all others. Sharing of passwords is strictly prohibited, and all passwords must be secured. Users are advised not to send their passwords through email or other electronic forms of communication such as SMS, or to write them anywhere in their offices. Users are advised to avoid using features such as "Remember Password" found in some applications, and passwords must only be used for the intended purpose. If a password is cracked or an account is compromised, the password must be changed immediately and ICT Directorate informed of the same, so as to institute investigations. From time to time, staff in the ICT Directorate shall attempt to hack into accounts as a measure of being a step ahead of the hackers, and users shall be advised immediately to modify passwords of those accounts that may be hacked into.

19.4 Characteristics of passwords

Passwords have different characteristics, features and strengths, and it is recommended that only strong passwords must be used always. Features of strong password include those with eight and above characters, together with a mixture of both upper and lower case characters, digits and characters such as +{-$<&}/}[>`|:@”? or ;\.!%*~. Weak passwords include family names, addresses, pets, phone numbers, friends, co-workers or words found in dictionaries. These also possess simple and easy-to-guess patterns like eeeee, ffffff, abcd, 12345 and these are highly discouraged.

20.0 Guidelines on Anti-virus

20.1 Purpose

These guidelines are intended to establish the steps to be undertaken by users of UoE ICT resources in detecting and preventing computer viruses.

Computer viruses can originate from files downloaded from the Internet, e-mails and/or email attachments. Viruses may also be transmitted by removable drives/devices such as diskettes, memory sticks, external hard drives, CD’s and DVD’s. Viruses are often files or email attachments that camouflage themselves as ordinary files or email attachments, and hence not very easy to detect.

In order to guarantee business continuity, the University has put in place measures to guarantee the ICT Devices, equipment and networks do not have viruses. It is the responsibility of every user to ensure that any ICT device or equipment connected to the University's network which is under their responsibility has working anti-virus software with suitable updates.

20.2 Introduction

It is expected that only genuine and licensed anti-virus software which is supported by the University is to be installed on UoE electronic devices, equipment and networks. The software must be activated to check for viruses as per schedule, and it must also be able to update automatically. Any user who creates and distributes malevolent computer programs, scripts or codes (Trojan horses, worms, viruses, email bombs among others) onto the UoE network shall be in violation of this policy. Users are advised not to open emails that are suspected to be viruses or considered to contain viruses as attachments, or to use computers infected with viruses. It is the responsibility of every user to notify ICT staff of such virus incidences, and any electronic device that has viruses or is reported to be infected shall be removed from the network until the incidence is fully attended to.

20.3 Regulations governing Virus Protection

To reduce chances of virus infection, all electronic devices connected to the UoE network shall be installed with standard anti-virus software supplied by the University. Users are advised not to access emails or messages with suspicious attachments/files or if they receive emails from a source which they do not know or trust. Users are further advised to be cautious with emails having suspicious website links or files with suspicious executable extensions (.exe) especially if they were not anticipating such website links or files. Users must also not download or install software from suspicious sources or from unknown/suspicious removable devices. Sharing of disks or removable media is highly discouraged, and all removable devices must be scanned before being used. Whenever a virus or a suspicious file is deleted, this must also be removed them from the 'Trash' folder as well as from the 'Deleted Items' folder to avoid any possibility of virus re-infection.

20.4 Responsibilities of ICT Directorate on virus Protection

The UoE ICT Directorate has the following responsibilities in relation virus protection:

(i) Advising the University Management on matters relating to virus protection and Anti-virus software.

(ii) Maintenance and updating of the Anti-Virus Policy guidelines.

(iii) Ensuring that anti-virus softwares installed on the University's computers are updated per schedule and that all anti-viruses are activated to update automatically.

(iv) Installation of anti-virus software on all UoE owned computer servers, desktop computers, laptops and workstations.

(v) Ensuring prevention and recovery following a virus attack.

(vi) Informing users of potential virus attacks and ensuring that reported virus attacks are addressed.

20.5 Responsibilities of UoE ICT Resources users on virus protection.

The following are some of the responsibilities of users of UoE electronic resources:

(i) All computers owned by Schools, departments and sections must have genuine anti-virus software installed.

(ii) All users must protect their computers against virus attack by following the measures outlined in this policy. They must refrain from changing or disabling anti-virus software installed on any electronic device connected to the University's network without seeking prior approval from the ICT Directorate.

21.0 Guidelines on ICT Equipment maintenance, repair, servicing and printing

21.1 Purpose

These policy guidelines outline the procedures for procuring, managing and replacement of ICT equipment within the University.

21.2 Introduction

From time to time, the University may need to purchase ICT equipment (hardware or software) to replace old and obsolete ones, damaged ones or even to buy new equipment using its own funds or from research or external funds. Whenever procuring an ICT related equipment or device for Departments, School, offices or sections, the ICT Directorate shall always be consulted for advice, and where necessary it may lead the process of procuring the ICT items.

21.3 ICT equipment classifications

(i) ICT equipment are either laptops, desktop computers, computer servers, printers, and monitors, audio-visual (AV) equipment, software and network equipment, telephones among others as described under ***Definitions*** and they do not include ICT consumables such as printer cartridges, CDs, DVDs etc;

(ii) ICT capital equipment are those that are registered in the University's Fixed Asset records and then given an asset number and are subject to depreciation;

(iii) Standard system include all components that are part of the standard package when a computer is purchased;

(iv) Custom system refers to all components chosen as part of a customized computer purchase;

21.4 Printing facilities

The University may consider establishing a centralized printing facility for most of the printing services. This facility shall contain at least a printer (preferably a network printer) which is controlled from a print server. The facility may also contain a photocopier for networked printing.

21.5 ICT Hardware and equipment Maintenance

The responsibility of managing, maintaining and servicing of all University's ICT hardware and equipment shall be vested on the ICT staff. This exercise shall be accomplished either according to the need or on a planned basis.

Further, the declaration of obsolescence of ICT hardware and equipment as well as giving a schedule of their disposal shall be done by ICT staff, following the University’s disposal procedures, the NEMA disposal guidelines and the University's Environmental Sustainability Policy.

21.6 Tools and equipment

Each section of the ICT Directorate shall be required to keep a suitable set of tools and equipment for repair, support and routine maintenance. For safety reasons, ICT staff involved in regular maintenance and support services shall be issued with suitable clothing and maintenance gear such as overalls, dust-coats and where necessary masks and gloves. They shall also be issued with appropriate communication tools to facilitate them to be in touch with each other during their work.

21.7 University workshops

The ICT Directorate shall maintain a well equipped workshop for repair and maintenance purposes at the main University and/or at the respective campuses.

21.8 Normal maintenance of ICT equipment

A timetable for Normal/ordinary maintenance of ICT equipments shall be developed by the ICT

Directorate following the advice/specifications of the respective manufacturers, and in some cases depending on the user's requirements.

21.9 Outsourcing Agreements of Services for specialized Equipment.

The ICT Directorate shall outsource the servicing, repair and maintenance of certain highly specialized and essential equipment whose support is not managed by the ICT Directorate.

21.10 ICT Hardware Obsolescence

ICT staff shall from time to time, conduct regular checks of ICT hardware and may declare some of this hardware as obsolete following expiry of its lifespan according to the manufacturers' specifications or according to procedure for replacement of ICT equipment as per this policy.

21.11 Equipment Warranties

ICT staff shall only participate in the repair and maintenance of ICT equipment as per their warranties, and when this is done, a documentation of all repairs and maintenance shall be done on each equipment and then kept by the ICT Directorate to be referred to in case the equipment is damaged within the duration of the warranty/guarantee.

21.12 Responsibility for monitoring conformity with ICT policies

The ICT Director shall ensure compliance with this policy, and shall report any breaches to the Vice-Chancellor. Such breaches may result in disciplinary action as per the University rules and regulations, and other relevant University disciplinary procedures.

22.0 Guidelines on General Procurement of ICT Equipment and Services

22.1 Introduction

From time to time, the University shall procure ICT equipment and services either to replace or to make additions to others. In making such purchases, the University's procurement procedures, policies, rules and regulations as well as other national regulations on procurement shall be adhered to. For all ICT related procurements, the ICT Directorate shall work in close consultation with the purchasing department, as well as advising the user departments in preparing the technical requirements. The ICT Directorate will give advice on the specifications of all ICT related equipment such as computers, laptops etc to be procured by users within the University.

It is the duty of every staff member wishing to procure ICT related services and/or equipment to familiarize themselves with this policy and other University policies dealing with procurement.

22.2 Objectives

1. To outline the processes to be followed during the procurement of ICT related equipment and services within the University.
2. To make users aware of their responsibilities while procuring or replacing ICT related goods and services.

22.3 Coordination of ICT equipment budget and procurement

Among other responsibilities stated in the statutes, the ICT Director shall be responsible for:

(i) Ensuring that the University maximizes on its purchases by clearly coordinating the University's ICT capital/central vote equipment procurement.

(ii) Advising users in the event of purchasing of an ICT equipment and ensuring that ICT capital equipment purchases are within the approved budgets.

(iii) Coordinating with the Deans, Directors, Heads of departments and sections, as well as other officers within the University in the preparation of the annual University's ICT capital/central vote expenditure budget.

The ICT Committee/board may also participate in advising on the annual ICT budget and procurements, together with proposing the manner in which priorities of ICT capital/central vote expenditure can be set, to the Vice-Chancellor for approval.

22.4 Capitalization of ICT equipment

Wherever possible, the Financial Management Information system and the fixed asset module of the Enterprise Resource Planning (ERP) system shall be used to evaluate the cost of each ICT capital equipment at a given time, in order to establish its lifespan.

All ICT equipment such as computer servers, desktop computers, laptops, monitors, printers and

AV equipment which constitute the pool of ICT equipment must be capitalized, regardless of their cost or their classification.

Capitalization shall exclude any other ICT equipment that is not categorized as per section 21.3.

22.5 Purchases through the ICT capital/central vote expenditure budget

Any ICT capital equipment that is not procured using Research or external research funds shall be bought using the University's ICT capital/central vote expenditure budget.

The ICT committee may from time to time be involved in authorizing the procurement of ICT capital equipment using the ICT capital/central vote expenditure budget.

22.6 Purchases through Research or external research funds

Any ICT equipment that is purchased through Research or external research funds is the property of the University and must be capitalized if it meets the criteria set out in section 21.3.

22.7 Purchase and replacement of ICT equipment

The University shall purchase ICT equipment and software through various Departments, Directorates, Schools, Offices or campuses. Members of staff who wish to purchase or replace ICT equipment must follow the established University procurement procedures and regulations regardless of whether the item is to be capitalized or not, or whether it's being bought with the University's own resources or research funds. The ICT Directorate shall provide specifications for all ICT related goods/services to be the procured.

(a) In the event that the Dean of a School, a Director, Head of Department or section or administrative office intends to purchase a new and/or to replace an ICT capital equipment, he or she shall be required to justify the need for such equipment for consideration by the ICT Director or ICT Committee or the Vice-Chancellor, unless such an equipment is to be bought using Research or external research funds.

(b) It is the responsibility of all users to ensure that before purchasing a replacement for an existing ICT capital equipment, such equipment is registered on the Fixed Asset Record and that it is marked as being ready for replacement.

(c) ICT capital equipment purchased through Research or external research funds is not to be replaced using the ICT capital/central vote expenditure budget.

(d) ICT capital equipment purchased with the ICT capital/central vote expenditure budget shall be due for replacement as per the replacement cycles established below:

(i) All desktop computers, including laptops: after 3 years;

(ii) Computer servers: after 3 years;

(iii) Computer monitors: after 3 years (those in high usage areas such as laboratories that are open 24 hours may have shorter replacement cycle, preferably after two and half years).

(e) Any user, member of staff or Council member issued with an ICT equipment such as a laptop, an Ipad, a cellphone etc, may only hold that equipment as long as they are in office or until such an equipment is declared obsolete, after which they shall hand it over to the Vice-Chancellor's office for issuance to the incoming user, member of staff or member of Council or for disposal.

Any ICT capital equipment that is to be replaced before its due date as explained in (d) above owing to either loss, damage or theft must be approved by the relevant Dean, Director, Head of department or section or the administrative officer concerned; if the ICT item is not insured, it shall be replaced using the ICT capital/central vote expenditure budget or through the votes of the concerned Schools, Directorates, Departmental or administrative office votes.

22.8 Management and security of ICT capital equipment

The ICT Director shall be responsible for ensuring that the following steps are taken to guarantee security of ICT capital equipment:

i) Asset numbers and labels are supplied and affixed on ICT capital equipments, and

ii) Serial numbers of ICT capital equipment are well captured and registered.

Deans, Directors, Heads of departments or sections or administrative offices shall be responsible for ensuring that the following is put in place within their areas of responsibility:

i) The proper asset labels are fixed on all ICT capital equipment in their areas;

ii) The correct site of the ICT capital equipment is recorded;

iii) Any disposal of ICT capital equipment is done following the guidelines for disposal of ICT Capital equipment, the Provision of Computers for Staff, Recycling, as well as guidelines for disposal of University Computers contained in the general University equipment disposal policy.

iv) Notify the University Security and other relevant security apparatus any theft of an ICT capital equipment.

Each School/department/section or administrative office shall be responsible for maintaining and repair of an ICT equipment that gets destroyed after the warranty period has expired.

23.0 Guidelines on ICT Training

23.1 Introduction

The University shall offer training to its staff from time to time, to empower them on new skills and also to update their skills continually with new ICT technologies.

Through the ICT Directorate, the University shall organize regular internal trainings to its staff and in some special cases to students on new ICT technologies. This shall enable the staff to carry out their duties effectively.

23.2 Objective

These guidelines are intended to ensure that staff are trained on relevant ICT skills within the University.

23.3 Structure of the Training

All the trainings offered within the University shall be planned, organized, implemented and conducted by the ICT staff. In some instances, where some Departments, Directorates, Schools or

Sections e.g. the Library wish to offer such services, this shall only be done in consultation with the ICT Directorate. In cases where the ICT Directorate does not have capacity to offer the trainings, the University shall collaborate with other external trainers/stakeholders to offer such training workshops. The training shall be offered to newly employed staff as well as other staff members who require such skills. The user Department shall choose the trainees to attend the training, as per their specific requirements.

However, although all staff within the University are expected to be computer literate, there may be those who are not. Members of staff falling in this category are encouraged to ask for training through their Heads of Departments, Deans, Directors or heads of sections or administrative offices to the ICT Directorate.

To offer quality training, the ICT Directorate shall develop a suitable ICT training curriculum to take care of both internal and external training on key ICT skills for those staff members who may be lacking in such skills. This curriculum shall be dynamic, and it shall progressively be updated to meet the challenges of the day. Where appropriate, the trainees may write an examination at the end of the training or do continuous assessment tests. The ICT Directorate shall also establish a state-of-the art computer laboratory for training purposes among others.

24.0 Statement of Implementation of the ICT Policy

The Vice-Chancellor has the overall responsibility of enforcing these policies in collaboration with the ICT Director. Each Dean of School, Director, head of Department or head of Section or head of an Administrative office shall ensure that this policy is enforced in their areas of responsibility.

Any violation of this ICT policy shall result into disciplinary action being taken against the responsible user according to the University disciplinary rules and regulations, other University policies and the relevant Kenyan laws.

25.0: Review

This policy shall be reviewed from time to time as the need arises, provided that two years shall not elapse before the last review.

26.0: Effective Date

This ICT policy shall come into effect on the date it is approved by the University Council.