SOUTH EASTERN KENYA UNIVERSITY

INFORMATION AND COMMUNCIATION TECHNOLOGY

POLICY

July 2014

TABLE OF CONTENTS

Abbreviations and Acronyms

CD ROM – Read only Memory Compact Disc
CD – Compact Disc
CDRW – Read/Write Compact Disc
DNS – Domain Name Services
FTP – File Transfer Protocol
ICT – Information and Communication Technology
ID – Identification Card
IP – Internet Protocol
IT – Information Technology
LAN – Local Area Network
LCD – Liquid Crystal Display
PC – Personal Computer
SEKU – South Eastern Kenya University
UPS – Uninterrupted Power Supply
WAN – Wide Area Network

Definition of Terms

Application software

Software that allows end users to accomplish one or more specific (not directly computer development related) tasks.

Database

Software used for management of data objects.

Hardware

All University -owned computer and peripheral equipment (such as printers, scanners, CD-ROMS (Read only memory compact discs), network cards and multimedia equipment). Excluded from such equipment would be equipment that is already under an existing service contract, warranty, nonstandard ICT equipment for which only advisory information shall be provided.

Software

Collection of computer programs and related data that provide the Instructions telling a computer what to do.

License

User right to use the software in the licensed environment.

Malware

Malicious software

Network

Group of computers and devices interconnected by communications channels that facilitate communications among users and allows users to share resources.

Operating System Software

Programs and data, which runs on computers and manages the computer hardware and provides common services for efficient execution of various application software.

Software

Collection of computer programs and related data that provide the Instructions telling a computer what to do.

Spam ware

Software designed by/or for spammers.

Spam

Use of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately.

System software

Software that helps run the computer hardware and computer system.

University

Refers to South Eastern Kenya University.

User

All University staff and students; any other organizations accessing services over University ICT resources; persons contracted to develop, repair or maintain University ICT resources; and suppliers of outsourced ICT services.

Virus

Software used to infect a computer.

CHAPTER ONE

1.0 GENERAL CONTEXT

1.1 Introduction

ICT resources at the University are intended to serve teaching, research and administration. The University grants members of the University community shared access to the resources as a way of accomplishing its vision and mission. Access to University ICT resources is a privilege. This privilege is extended to all faculty, staff and students and may be limited or revoked if the user violates the set out guidelines for use. All users are expected to use these resources in an effective, efficient and responsible manner so as to realize optimum benefit from the facilities.

The University has the responsibility of ensuring the ICT resources it has provided are used for the purposes they are intended. For this reason, the University has set out this ICT policy as a guideline for effective use of these resources. The policy aims to identify ICT services incorporated within the University ICT infrastructure and define a governance and management structure. It articulates the policy guidelines and framework as program actions adopted by the University for implementation and use of ICT and describes critical areas for the development and application of ICT by laying out the blueprint in terms of the University's strategy on using ICT as an enabling tool.

Additional policies may be issued from time to time to support this policy. All members of the University community will be expected to be familiar with and comply with this policy.

1.2 Vision

To become a Centre of Excellence where the potential of ICT is harnessed to serve as a catalyst for effective teaching, research, and replenishment aimed at the promotion of innovation in education technology and transforming lives.

1.3 Mission

To use ICT optimally with the view to increasing efficiency among both staff and students and

endeavour to fit into the new global information and knowledge based economies.

1.4 Goals

This policy establishes a regulatory framework and guide for developers and users of ICT resources on appropriate standards to be adopted at the University.

1.5 Scope

This policy applies to any person accessing, developing, implementing and/or using ICT-based information and ICT resources owned, managed, supported or operated by, or on behalf of, the University. The addressed include all University staff and students; any other organizations accessing services over University ICT resources; persons contracted to develop, repair or maintain University ICT resources; and suppliers of outsourced ICT services.

1.6 Objectives

This policy has been established to:

1) Provide guidance in the development, use and maintenance of a reliable, secure and cost effective ICT infrastructure.

2) Assure the confidentiality, integrity and availability of information within University.

3) Make ICTs accessible to the University community regardless of gender, age, religion, location and race.

4) Enrich learning for students and effective content delivery for staff through use of ICT.

5) Ensure the establishment of an efficient ICT environment that provides for collaboration and sharing of information over University networks.

CHAPTER TWO

2.0 FUNCTIONS OF THE ICT DEPARTMENT

1) Implementation of the ICT Policy
2) Undertaking needs assessment on the ICT equipment with a view of helping in procurement and maintenance as deemed fit
3) Capacity building: Basic Computer Literacy training
4) ICT Helpdesk services: These include:
    a. Hardware trouble shooting and maintenance
    b. Software installation
    c. Computer peripherals installation and servicing
    d. Network administration
5) Website maintenance
6) Implementation of Information Systems in the University
7) In charge of ICT requirements especially on matters related to technical advice on ICT initiatives in the University.

To realize the above functions, the following policy guidelines have been established.

CHAPTER THREE

3.0 INVENTORY AND EQUIPMENT USE POLICY

3.1 Introduction

Information Communication Technology (ICT) is based on the correct use and deployment of suitable and sufficient ICT Equipment and software infrastructure.

3.2 Hardware

These include but are not limited to:-

1) Personal Computers
2) Laptops
3) Printers
4) Scanners
5) Computer Servers
6) Power Backup Equipment (UPS)
7) L.C.D Projectors
8) Network Equipment
9) Digital, Camera / Cam coders
10) Removable media
11) Photocopiers

3.3 Software

These include but are not limited to:-

1) Network Operating Systems
2) PC Operating Systems
3) Application Software
4) Antivirus Software
5) In-house developed Systems
6) Off the shelf Systems

The ICT Department shall be responsible for keeping up to-date inventory of the hardware and software that is in use by the University. The Department will ensure that:-

1) The hardware installation has sufficient capacity to serve the University
2) The University uses current technology in all areas of operations
3) The operating software runs continuously well and without failure.
4) The application software consistently provides the user with appropriate reports for decision-making
5) The hardware and software are used properly as intended
6) That the licensed software in use is renewed
7) That only the right personnel use the computer equipment. Any other personnel to be authorized by ICT Department
8) That the hardware and software are well maintained and periodically revised to consistently meet the set objectives

CHAPTER FOUR

4.0 THE USER POLICY

4.1 Introduction

The policy is based on the following principles, which must be adhered to by all persons responsible for the implementation of this policy and to whom this policy applies:

1) The ICT resources of the University shall be provided to support teaching, research and administrative activities of the University in line with its mandate.
2) Authorized users are required to familiarize themselves with the University ICT Policy.
3) Only authorized users shall be granted access to University ICT resources and it will be their responsibility to ensure that these resources are used with regard to this policy.
4) Users shall be required to complete a Compliance Form prior to authorization being granted for access to ICT Resources.
5) The University may inspect, without notice, any data on any resource owned by the University (regardless of data ownership), including electronic mail and other forms of communication.

4.2 In Making Acceptable Use Of Resources Users Must:

1) Respect the rights, privacy and property of others.
2) Scan any removable media with Antivirus before using them on computer systems.
3) Obtain official e-mail addresses from the ICT Department whose ownership must not be transferred to a third party.
4) Ensure the security of their workstation by logging off or locking it when it is left unattended.
5) Access only information that pertains to them, that which is available to the public

and/or to which they have been granted authorized access.

6) Use the ICT resources in appropriate, responsible, ethical and in a lawful manner.

7) Ensure that requisite approval is sought from ICT Director before any removable media containing University data are released to any other external party.

4.3 In Making Acceptable Use Of Resources Users Must Not:

1) Use University resources for private commercial purposes.

2) Deliberately interfere with or gain illegal access to user accounts and data including: viewing, modifying, destroying or corrupting the data belonging to other users.

3) Making unauthorized changes to the setup or configuration of software or hardware.

4) Utilize the University ICT Resources to play computer games, movies or any other form of entertainment.

5) Deliberately impede other users through mass consumption of system resources.

6) Use computer programs to decode passwords, encrypted data or access-control information belonging to other users.

7) Purposefully scan internal or external Computer Systems in an attempt to discover or exploit known computer software or network vulnerabilities.

8) Install any software or hardware as that remains the preserve of ICT personnel.

9) Use University ICT resources to harass or intimidate other persons, for example, by broadcasting unsolicited messages, by repeatedly sending unwanted mail.

CHAPTER FIVE

5.0 INTERNET POLICY

5.1 Introduction

Internet has become a great enabler in the knowledge acquisition process especially in the academic field. Internet can be a double edged sword if proper regulatory measures are not put in place. This policy seeks to govern the use of Internet at the University ensuring that all users engage in legitimate use of Internet.

The policy is based on the following principles, which must be adhered to by all those responsible for the implementation of this policy and to whom this policy applies:

1) The Internet shall be used to increase staff and student access to information on matters related to the support of education and research.
2) Users of privately owned mobile systems shall obtain IP Addresses from the ICT Department upon filling a request form.
3) All files downloaded from the Internet shall be scanned for malware using the University anti-virus software with the latest virus detection updates.
4) All Internet access software shall be configured to use stipulated gateways, firewalls, or proxy servers. Bypassing any of these servers shall be strictly prohibited.

5.2 In Making Acceptable Internet Usage, Users Must Not:

1) Use University Internet infrastructure for non academic and unofficial purposes.
2) Transmit University data over the Internet without the approval of the ICT Department.
3) Using any program, script or command, or sending messages of any kind, with the intent to interfere with, or disable, another user's terminal session, via any means, locally or via the Internet, intranet or extranet.
4) Use the University Internet resources to spy on other internal or external network users.

CHAPTER SIX

6.0 EMAIL POLICY

6.1 Introduction

The email policy provides guidance on acceptable email user practices, for the purpose of sending and receiving email messages and attachments on ICT facilities provided by the University .

It is important to note that the University staff and student email systems are key communications systems in the institution. Inappropriate use of the email system can lead to malware infection, which ultimately could lead to degradation of network performance and in extreme circumstances crush the entire University system. Email account access will cease on expiration of contract, services or course programme duration.

6.2 Acceptable Use Include But Not Limited To

When using the email or messaging system, users must at all times:

1) Respect the privacy and personal rights of others.
2) Take all reasonable care not to plagiarize another person's work; or defame another person.
3) Users shall not open e-mail attachments received from unknown senders, as it may contain malware.
4) Users will be required to immediately log off from their email account after use.

6.3 Unacceptable Use

When using the email or messaging system, users must:

1) Not send offensive, intimidating, harassing or humiliating emails to other persons.
2) Not create or transmit material that includes false claims of any deceptive nature.
3) Not forward or otherwise copy an email belonging to another user (except with their permission) or an email which contains other users personal information.
4) Not send forged messages, obtain or use someone else's e-mail address and password without their authorization.
5) Not send spam.
6) Not send sexually explicit material.

6.4 Disclaimers

The University may from time to time arrange for an appropriate disclaimer to be appended to all email messages that are sent to external addresses from the University, in order to provide necessary legal protection.

CHAPTER SEVEN

7.0 HARDWARE AND DATA SECURITY POLICY

The ICT Department will be responsible for complete hardware and data security of the University .

7.1 Hardware Security

To ensure proper and continuous operation, the following hardware security measures shall be observed:

1) Servers, PC's and network devices to be installed in secure and well ventilated rooms and supplied with sufficient power through proper rated UPS.
2) To avoid virus infection, use of removable media should be subjected to virus scan before use.
3) Provision of sufficient warranty on all computer hardware in use.
4) Entry to the Server Room shall remain restricted to ICT Department staff.
5) Movement of ICT infrastructure within or out of the University must be authorized by the ICT Director.
6) All personal ICT infrastructures must be registered by the ICT Director.

7.2 Data Security

Due to importance of data in any given enterprise, the ICT Department shall take regular backups and any other security measures to ensure that the University data is safe and can be relied upon in the event of data loss.

The following security measures shall be taken to safeguard University data:-

1) Plan for recovery or restoration in the event of a disaster.
2) The ICT Department will keep proper backup of data in the University database. The data backup will be on daily basis and retained for a period of up to one week. Weekly, monthly and annual backups shall be kept appropriately for future reference.
3) Due to the frequent change in technology, the backup's media shall be revised consistently to ensure that all the backups are accessible and can be redeployed when needed.
4) The backup media shall be kept in the designated fire-proof safes both onsite and offsite.
5) These procedures shall be revised from time to time to ensure minimum downtime in the event of data loss.

CHAPTER EIGHT

8.0 PASSWORD POLICY

8.1 Rules

Access to the computer network is only possible through a user having a correct username password. Passwords are like keys to a safe hence the following standards of security shall be observed by users:-

1) Obtain usernames and passwords when needed and to memorize passwords.
2) Users are held accountable for their password and should not share them.
3) Passwords shall be kept confidential and not posted in public view.
4) Passwords shall not be inserted into email messages or other forms of electronic communication, except at the initial opening of the email accounts by ICT personnel.
5) Users shall not use the "Remember Password" feature of applications like Mozilla Firefox and Internet Explorer.
6) Report to ICT Department incase of forgetting password for a reset.
7) To avoid simplicity and to enhance University security, the passwords shall be 8 characters and above, and are recommended to be changed periodically.
8) For security reasons no user shall be allowed to operate the network servers or use administrative passwords without permission.
9) Servers and other administrator passwords are to be kept by ICT Director and copies kept by the ICT personnel in charge.
10) Users who are no longer members of the University community will have their usernames and passwords revoked immediately.

CHAPTER NINE

9.0 INFORMATION POLICY

9.1 Introduction

All members of the University community have a responsibility to protect information from unauthorized generation, access, modification, disclosure, transmission or destruction. Any member of the University community who comes across any evidence of information being compromised or detects any suspicious activity that could potentially expose, corrupt or destroy information must report such matter to the University ICT Director. No one should take it upon himself or herself to investigate the matter further without the authorization of the University ICT Director.

The purpose for this policy is to educate the University community about the importance of protecting information generated, accessed, transmitted and stored, to identify procedures that should be in place to protect the confidentiality, integrity and availability of University information.

9.2 Responsibilities for Information Management

1) Protect University information so as to ensure its confidentiality, integrity, and availability.
2) Use the information only for approved University purposes.
3) The user must not in any way copy, release, sell, loan, review, alter or destroy any information except as properly authorized within the scope of the user's professional activities.
4) The user must safeguard any physical key, ID card, computer and/or network account that allows access to confidential information.
5) Before systems or media are reused they should be erased accordingly to ensure no residual data.

9.3 Classification of Information

University classifies information into the following three categories:

1) Public
2) Official Use Only

3) Confidential

This policy presumes all data is public, unless specifically classified as Confidential or Official Use Only in accordance to regulations regarding privacy and confidentiality of information.

Public Information

Information to which the general public may have access to include, but not limited to:

1) Publicly posted press releases
2) Publicly posted schedules of classes
3) Posted interactive University maps, newsletters, newspapers and magazines
4) Telephone directory information
5) Information posted on the University's College Web site
6) Publicly posted meeting announcements and agendas

Public information should be released by authorized persons only.

Official Use Only Information

The information must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage or other use. Official Use Only information is restricted to certain employees of the University who have a legitimate purpose for accessing such data.

Official Use Only information:

1) Must be protected to prevent loss, theft, unauthorized access and/or disclosure.
2) Must be stored in a closed container (i.e. file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use.
3) Must be stored in a non-publicly accessed server / drive.

Confidential Information

Information that, if disclosed to unauthorized persons, would be a violation of the information policy. Any file or data that contains personally identifiable information of an officer, administrator,

school, staff, retiree, student, graduate, donor, or vendor may also qualify as confidential information. Some examples of confidential information include, but are not limited to:

1) Medical records of any kind
2) Student records
3) Unique identifiers such as National Identification Numbers
4) Benefits records
5) Retirement documents
6) Payroll records

Confidential information:

1) Must be stored in a secure location which has sufficient physical access control measures to provide adequate protection and prevent unauthorized access.
2) When stored in an electronic format, it must be protected with strong passwords and stored on servers that have protection and encryption measures in order to protect against loss, theft, unauthorized access and unauthorized disclosure.
3) When sent electronically, it must be to a previously established and used address or one that has been verified as a secure location.
4) Must not be posted on any website.
5) All confidential data, electronic or printed, and data containers (e.g. filing cabinets, servers, and magnetic or optical storage media) must be clearly labeled.
6) Must be destroyed when no longer needed subject to the University's College Records Management policy.

CHAPTER TEN

10.0 TELEPHONE POLICY

10.1 Introduction

This policy and the associated rules apply to all University telephone services. All users should be aware of the policy as well as their responsibilities and legal obligations. To ensure proper and continuous operation, the following measures shall be observed;

1) The University shall endeavor to avail telephone services to all staff and faculty through a central telephone exchange centre.
2) The University has the right to replace or change any number necessary due to any constraints.

10.2 Telephone Use

1) Use of University telephones for personal calls is not encouraged.
2) Telephone facilities for students' societies and laboratories are restricted to internal calls only.
3) The University reserves the right to monitor the destination, volume and duration of all calls to the University phones in support of its mission and to investigate complaints.
4) The University has the right to disconnect any extensions where it deems necessary.

CHAPTER ELEVEN

11.0 NETWORK POLICY

11.1 Introduction

ICT networks are a critical component of the University infrastructure. They offer the backbone of sharing resources and communication channels necessary to facilitate the core functions of the University mission. The University shall ensure that ICT networks are robust, resilient and have adequate security, redundancy and backup. The ICT network infrastructure shall integrate data, voice and video.

The Network Policy establishes a guideline for the management of all networks in the University. It defines the arrangements and responsibilities for the handling, maintenance and use of ICT networks. The policy applies to any person accessing or using the ICT network owned, managed, supported or operated on behalf of the University. These include but are not limited to all University staff, students, persons contracted to repair or maintain the University's ICT networks and suppliers of network services.

11.2 Handling of ICT Network Equipment

1) Only designated ICT personnel are authorized to install and maintain active network equipment of any nature connected to the University ICT network.
2) Where ICT Director agrees that academic staff or the ICT personnel may install and maintain local staff and student networks, such permission will exclude the point at which these networks connect to the University's ICT infrastructure.

11.3 Connecting to the ICT Network

All connections to the University Computer Network shall be governed by the following principles:

1) Any computing device that is connected to the University network should be properly protected against hacking, viruses and similar security threats, through appropriate use of security technology, including anti-virus software.

2) Users of portable computer devices who wish to directly connect to the University

network are required to register their computer with the ICT Department.

3) No data communications device may be directly connected to a network access point without the prior approval ICT Director or a person acting on his/her behalf.
4) No computing device may be directly connected to the University network while at the same time connected to external network.
5) All connections to the University's ICT networks must conform to University Internet Protocol (IP) addresses.
6) The University reserves the right to limit access to its networks if there is suspicion of violation of the network policy.
7) Personal computers which house material which violates the University ICT policies can be subjected to network disconnection without notice.
8) Personal Computer Systems connected to the University network shall not be set up to offer services to other users, for example, to act as servers, unless the prior written consent of the ICT Director has been obtained.

11.4 Use of the Network

1) The University network must not be used for purposes other than academic, research and administration.
2) Users may not run network applications in such a way as to deny network access to other users or jeopardize, in any way, the integrity, performance or reliability of University Computer Network.
3) User shall not steal or vandalize any University network equipment.
4) Any effort to circumvent the wired or wireless computer network security systems designed to prevent unauthorized access may result in the suspension of all access and an appearance before the appropriate disciplinary committee.
5) If a member of staff requires a new service or one that has been previously made unavailable, their first request should be to ICT Director. Students should pass their requests to their lecturers who should pass these requests on as above.
6) Under no circumstances should unauthorized persons disconnect other equipments for whatever reason.

11.5 External Access to University ICT Network

Where specific external access to University computer network is required, ICT Director shall ensure that this access is strictly controlled and limited to specific external locations or persons.

11.6 Domain Name Services

1. All Domain Name Services (DNS) activities hosted within the University shall be managed and monitored centrally by the ICT Department.
2. Services provided by members of the University community as part of their official functions will be registered within the University domain.

CHAPTER TWELVE

12.0 ICT TRAINING POLICY

12.1 Introduction

It shall be mandatory for all University staff to be ICT literate, the level of ICT literacy being in line with the demands of their job functions. Training shall therefore focus on building skills in users to make them effective in exploiting provided ICT resources. Continuous training of staff on upcoming technology is emphasized.

To ensure that users have sufficient knowledge of operating computer systems, current technology and job demands: -

1) Internal ICT user training targeting the University community shall be scheduled on a continuous.
2) External ICT training shall be organized by the ICT Department in response to need as may be assessed from time to time when training is not possible within the University.
3) The University shall facilitate training of ICT staff consistently to act as the first level ICT support and to champion ICT in the University.
4) The University shall provide relevant learning materials on ICT in the ICT Department.

12.2 Administration of Training

1) Every section head or person in charge of a section shall in response to needs assessed, nominate staff to be trained biannually and forward the list to ICT Director. The number of staff to be trained shall be as targeted in the Strategic Plan for the University. The University shall make the necessary arrangements to facilitate trainees drawn from such Departments.
2) The University shall provide necessary resources to facilitate the training.
3) The ICT Department shall develop topics for all training including development or sourcing of training material. These shall include but are not limited to:-
    a. Where possible provide training materials on-line via the University website or intranet.
    b. Where possible conduct on-line assessment tests and examinations via the University intranet.

4) The ICT Department shall where possible issue certificates on successful completion of training and assessment tests.

CHAPTER THIRTEEN

13.0 COPYRIGHT POLICY

1) Members of the University community must abide by the terms of copyright laws, software licensing agreements and contracts that pertain to the University's ICT resources.

2) The University shall not allow the use of software that does not have a license. Any user found using unlicensed software shall be reported to ICT Director for disciplinary action.

3) Use of electronic resources such as databases, online journals and e-books provided by the University is governed by individual license agreements and is for non-commercial research and study purposes only.

4) Users of the University shall not download, store and/or disseminate copyrighted materials including software and all forms of electronic data without written permission of the copyright holder.

5) Posting any copyrighted material, registered trademarks, brand names or other protected symbols in an electronic form that is accessible by others within and outside of the University community, even if for the purpose of personal use without written permission of the copyright holder is in violation of law and is prohibited.

6) Any graphics, multimedia programs, instructional material or articles produced wholly or in part using the University ICT resources shall remain the Copyright and intellectual property of the University .

7) Users shall not be allowed to sell or distribute any copyrighted materials belonging to the University without authorization.

CHAPTER FOURTEEN

14.0 ENFORCEMENT OF THE ICT POLICY

1) Alleged or suspected violations of this Policy shall be reported to the ICT Department. Unlawful use of ICT resources and equipment is subject to disciplinary action, which may include temporary suspension of these privileges and other disciplinary sanctions up to and including termination of services.

2) Unlawful use of ICT resources may also lead to criminal or civil legal action being instituted against authorized individual users as the case may be.