KILIMANJARO CHRISTIAN MEDICAL UNIVERSITY COLLEGE

Information and Communication Technology (ICT) Policy

Summary: This ICT POLICY is designed as a guideline governing the use of Kilimanjaro Christian Medical University College (Hereinafter to be referred as KCMUCo) Information and Communication Technology Resources. It outlines the guidelines that should be applied to Information and Communication Technology within or by the Institution.

FOREWORD

The KCMUCo ICT Policy was formulated in 2016 to guide the identification, promotion and appropriate utilization of ICT and ensuring that ICT applications are integrated into the planning and College strategic plan.

Information and Communication Technology (ICT) is fundamental in facilitating KCMUCo core functions i.e. teaching, research and Service. The importance of ICT in innovation for knowledge generation and technology transfer geared at enhancing national development as a component of Education for life has been embraced in the College strategic plan.

The purpose of this Policy is to assist researchers, research managers and KCMUCo in ensuring that they have access to best practices for the identification, protection and management of ICT. Furthermore, the implementation of this policy is expected to enhance the visibility of KCMUCo and hence improving the performance of the College.

KCMUCo, therefore, affirms its commitment to adopt and operationalize e government standards; ensure availability of Internet bandwidth, improved ICT Infrastructure, ensure that anti-virus updates, and data back-up are in place; Increase the percentage of staff who have access to broadband and Internet in the work place. KCMUCo further acknowledges the importance of and shall support ICT utilization in service provision, research and innovation.

Prof. Egbert Kessi
Provost
Kilimanjaro Christian Medical University College

February, 2016

KILIMANJARO CHRISTIAN MEDICAL UNIVERSITY COLLEGE

PREAMBLE

Information Communication Technology (ICT) has become the backbone of day to day operations in almost all organizations. KCMUCo is not an exception. Organizations/ Institutions all over the world, including KCMUCo, are faced with the challenges of ICT security and establishment of acceptable use of ICT as well as legal compliance.

KCMUCo recognizes its responsibility to utilize technology and to facilitate wide participation in this effort to develop a meaningful policy, which seeks to articulate the principles and guide the actions required to fully utilize the available information and communication technologies.

This ICT Policy document therefore seeks to provide guidelines for compliance, acceptable and secure use of information communication technology by KCMUCo staff, students, Volunteers, and other important College stakeholders.

KCMUCo understand that, the comprehensive choice of ICT for holistic development of education can be built only on a sound policy. The initiative of ICT Policy in College Education is inspired by the tremendous potential of ICT for enhancing outreach and improving quality of education. This policy therefore endeavors to provide guidelines to assist KCMUCo in optimizing the use of ICT in College education and maintaining its education standard.

The ultimate purpose is for more effective creation and delivery of educational products for improved teaching and learning in KCMUCo.
With the convergence of technologies, it has become imperative to take a comprehensive look at all possible information and communication technologies for improving education in the College.

ACKNOWLEDGEMENT

It is with great honor to thank the Almighty God for having made possible the development of this policy. We would like to express our deeply appreciation to the management of Kilimanjaro Christian Medical University College for the support shown to us while developing this policy.

This ICT policy has been developed for purpose of mitigating challenges faced in today's world of science and technology.

Special thanks go to those who were engaged in evolving this policy including Mr. Frank Dubi, Mr. Gabriel Msuka, Mr. Deodatus Mogella, Mr. Fadhili Ndimangwa, Mr. Amani Minja, Ms. Glory Ibrahim, Ms. Dativa Tibyampansha and Mr. Aniceth Boyi.

THE RATIONALE OF THE ICT POLICY

1. A good policy protects both the employer and employee from misuse of files, applications, the Internet, email and other electronic interfaces. With the rapid evolvement of the Internet and related systems there has been enough scope for misuse. Therefore, this ICT policy is very useful in regulating behavior of the users.

2. It must be clearly understood that KCMU College should protect itself and its employees and properties from misuse. This policy ensures that misuse is controlled. However, it must be understood that the aim of this policy is not only restrictive, but also is very useful to the employees by providing guidance.

3. College realizes that the private actions of the employees in the system might be confused with those of the employer. Therefore, the consequences of the association between the College and the user could and should not be allowed to be detrimental to the College.

ABBREVIATIONS AND ACRONYMS

AMIS	Academic Management Information System
CCTV	Closed-circuit television
CITI	Collaboration Institutional Training Initiative
DPA	Deputy Provost Administration
DPAA	Deputy Provost Academic Affairs
ICT	Information and Communication Technology
IRB	Institutional Review Board
KCMUCo	Kilimanjaro Christian Medical University College
PC	Personal Computer
MDGs	Millennium Development Goals
LCMS +	Learning Content Management System Plus
WAN	Wide Area Network
MOOC	Massive Open Online Courses

Table of Contents

DEFINITION OF TERMS

In this policy, unless the context otherwise requires: -

"Computing devices"	Laptops, desktops, tablets, mobile phones;
"Dspace"	Dura Space;
"E-mail applications"	Outlook, my Mail, Thunderbird;

"Information and communications technology (ICT)" to all the technology used to handle telecommunications, broadcast media, intelligent building management systems, audiovisual processing and transmission systems, and network-based control and monitoring functions. ICT has more recently been used to describe the convergence of several technologies and the use of common transmission lines carrying very diverse data and communication types and formats;

"ICT venues"	Computer lab, E-library and Faculty room;
"Moodle"	is free and open-source software learning management system;
"Network devices"	Routers, Switches, Bandwidth Controllers, Firewalls, IP phones;
"Printing devices"	Scanners, fax, Copiers, and Printers;
"Office packages"	Word, Excel, Publisher, Outlook, PowerPoint (Microsoft, Mac, Linux).

KILIMANJARO CHRISTIAN MEDICAL UNIVERSITY COLLEGE

1. INTRODUCTION

Information and Communication Technologies (ICT) are now widely accepted by developing countries as a critical tool in their efforts to eradicate poverty, enhance human development, and achieve Millennium Development Goals (MDGs). Recognizing this untapped potential, infrastructure initiatives and development strategies incorporating ICT are being increasingly promoted and launched across Tanzania.

To understand the role that ICT can play in human development, there is a need to first understand the requirements and circumstances of the people who are to benefit from the introduction of ICT. At the same time, the ways in which ICTs can help people to meet these needs to be understood.

The extensive use of computers and other ICT equipment is highly encouraged and used in provision of services at KCMU College. Computers are widely used for administration and communications purposes and increasingly used as tool for provision of services. Though ICT systems can be used for the enhancement of productivity and services, it is also vulnerable to accidental or deliberate misuse.

This Policy sets out guidelines on the use of ICT systems and the consequences for non-compliance.

The Policy applies to all the KCMU College employees, contractors, consultants, agents, students and any other person who use or have access to email or files, software applications and the Internet during the course of their employment or business dealings with the KCMU College, whether such use takes place on the KCMU College premises or elsewhere.

The purpose of this Policy is to put into place guidelines for the use of computers and access to files, email and Internet systems by the users of the system.

1) Aim of the ICT Policy

To support the strategic vision of the College by improving operational efficiency and exchange of information so as to maintain a competitive edge.

2) Specific Objectives

The specific objectives of the College ICT policy are to:

a) Provide cost effectively information and communication technology facilities, services and automation;
b) Improve on customer satisfaction;
c) Identify priority areas for ICT development;
d) Encouraging innovations in technology development, use of technology and general work flows;
e) Help people to adapt to new circumstances and provide tools and models to respond rationally to challenges posed by ICT;
f) Promoting information sharing, transparency and accountability and reduced bureaucracy in operations.

3) Applicability and Compliance

All staff, students, part time staff, volunteers etc and all sections, units, departments, faculties, and Directorates shall be required to comply with the provisions of this Policy.

4) Principles

This policy shall be guided by the following key principles:

a) Mainstreaming of ICT in the College;
b) Seamless integration of ICT;
c) Inclusion, flexibility support to all stakeholders in the College and management system;
d) Adherence to best practices & policies;
e) Economies of scale and customer value propositions.

5) Policy Statements

In order to ensure focused implementation of ICT policy the following articles of policy statements are hereby declared:

a) Assure availability of all anticipated ICT services/systems at all workplace in the College;
b) Assure availability and controlled usage and changes of basic User-level Data Communication and telecommunication Services such as e-mail, Access-to-Internet/Extranet/Intranet services and telecommunication terminal equipment which actually are major 'elements' of the low-level network & communication Services;
c) Promote office computing in all offices. This applies to lecturers, researchers, administrators, managers, as well as to secretarial and clerical workers. Major office computing applications are: office packages, electronic e-mail, data and document storage and retrieval desktop publishing, access-to Internet and intranet;
d) Continuously improve both the efficiency and effectiveness of library operations and services through the implementation of an integrated on-line library information system;
e) Enhance and streamline education related administrative and managerial processes and to improve academic reporting through the implementation of an integrated academic records information management system;
f) Enhance and streamline financial management processes and reporting through the implementation of an integrated financial information management system;
g) Enhance and streamline the human resource management and administrative processes through the implementation of a human resource information system;
h) Enhance and streamline the property and asset management and administrative processes through the implementation of an asset and inventory information system;

i) Enhance and streamline procurement management systems;
j) Harness ICT potential in enhancing online and distant learning in order to maximize flexibility in education and reach out to a wider coverage of prospective learners;
k) Ensure that students and staff are trained on a continuing basis to equip them with the requisite skills to fully exploit the ICT potential in their different functions, in order to make the entire College fraternity "ICT – Complaint".

l) Ensure sustainable management of the institution's ICT resources through creation of appropriate policy guidelines and regulations, advisory and operational organs that will cater for the broad interests of all users;
m) Provide for the growth of its ICT resources and their financial sustainability through adequate funding and appropriate operational mechanisms.

2. System Integrity and Support

Users shall not be allowed to disconnect PCs or other ICT equipment, from the main supply or from network connection points; doing so may corrupt data stored on the system or the current work of other users. Always the user shall contact ICT support if there is a need to move any piece of ICT equipment for any reason whatsoever.

3. Data Security

1) There shall be networks with central file servers where all data files of whatever kind shall be stored. Every user shall have "user account" on the network in the establishment where they work, which can be accessed from any computer connected with Internet. The user account shall provide secure connection to the network via a password. As part of their user profile, each user account shall possess a reserved space on the data server where his/her data files can be stored in privacy.

2) Users shall always be required to save their work in central file server. Never attempt to save work on the "Desktop" or on the local "C-drive". User may create as many sub-folders within as he/she wish to assist in the organisation of the work. The contents of the file servers are backed up on a routine daily basis; saving your work in centralised file server protects you from the loss of valuable information should there be a hardware failure in your PC. Data saved in any other way is not backed up, and will be lost if your machine suffers a mechanical breakdown.
3) Please remember the deleted files do not work with network storage. Once a file is deleted, there is no easy way for it to be recovered. If you unintentionally delete a file, which is required, Contact the ICT Directorate's support person immediately. It may be possible to recover lost data if action is taken quickly. The longer the matter is left unreported, the greater the likelihood the data will be irretrievable. If a lost data file was in existence the day before deletion, it may be possible to recover the earlier version from the backup files.
4) Users should take precautions to protect access to their data and work files. Although machines have screen savers which blank the screen after there has been no activity for a prescribed period, which requires your password to be entered to return to existing work, you should not rely on this if you are intending to be away from your desk for any significant period. Anyone in the surrounding area could get to the machine once you have vacated your workstation prior to the screen saver starting, and then have access to all your data. Depending on how long you are planning to be away from your desk, when you leave your desk for any reason you should:

    a) Log off or Lock the machine.
    b) Turn off the machine (Applies when you are leaving for the day)

5) Many networks contain public folders and files, for material, which needs to be available to more than one user. You should never modify the public folder structure unilaterally; this may

cause other users to lose access to their work. If you consider that the folder structure should be modified, consult your ICT support person, so that the impact of the proposed changes can be assessed and other users consulted.

6) The computer system and its networks are provided for KCMUCo business purposes only. You should not create any personal files or store personal data on the system.

4. Computer users

1) It is the responsibility of the user to ensure that amended documents or data are saved back to the network for the security of data. Ideally the use of shared folders, network files facility (which ensures that the contents of the laptop are synchronised with the network) is the preferred way of ensuring this.

5. Passwords

1) Passwords shall be required for various applications and access to systems. For system security these passwords shall be required to be changed from time to time. Passwords must have at least 8 characters, including alphanumeric and special character.
2) It is the responsibility of users to ensure that personal passwords are not shared or disclosed to any other users. If you believe that someone else knows your password, please change it immediately.
3) Never share your password with colleagues for any reason. There may be times, such as holidays or other periods of extended absence when it would be useful for other users to have access to data that you store in your area. Do not do this by sharing passwords. Each network file server has a public folder which all users can access based on rights assigned or requested by Department head. Documents which are not confidential can be stored or copied here and accessed by other users.

4) If you wish to share confidential work with one or more trusted colleagues, your system administrator can create a private shared space which only nominated people can access where confidential files may be shared.

6. Viruses

1) Viruses can be introduced into the KCMUCo's systems and networks or transmitted to a third party's system by sending and receiving email and by using the Internet or exchanging files using external devices. The deliberate introduction of a virus is a criminal offence.
2) Accidental introduction of viruses may, in certain circumstances, give rise to a claim against the KCMUCo. All users shall take reasonable steps to ensure that no viruses are transmitted and must follow the KCMUCo anti-virus procedures.
3) Viruses may also be introduced when data is imported to the KCMUCo systems using Compact disc (CD), USB flash drive, external hard drives and similar devices. Any user who imports material prepared on their personal computer equipment or other third party system must ensure that the system used to prepare or amend the material is fully protected by a recognised anti-virus programme, which is kept fully up to date.
4) Personal unregistered equipment (laptop computers, digital players, digital camera etc) must not come into contact with the network. Users must not attempt to connect any of their own personal equipment direct to network connections or to connections on KCMUCo owned computers. This restriction applies to hard-wired connections to data sockets and connection via wireless access points where these exist.
5) The restriction on connecting digital devices is because of the multiplicity of software, which could be required. Every establishment has a multi-format card reader - to transfer pictures or files.

7. Backup and Recovery

1) In order for the backup policy to work effortlessly only the office packages shall be taken for backup.

2) Back-up procedures, ensuring that both data and software are regularly and securely backed-up, are essential to protect against loss of that data and software.

3) ICT team members shall ensure a daily incremental and a weekly backup to the backup servers, for the purpose of restoring a system in the event of a system failure. In any absence of a responsible ICT member(s) then, other ICT member(s) should take responsibility of backup. In the event of a disaster IT personnel shall work hand in hand to restore user files but does not guarantee retrieval. The responsibility for backing up user files remains with the user. However, ICT members should undertake all possible measures to ensure that backing up user files is accurately undertaken and proper operations of the baking up system.

   If ICT staff should have occasion to deal with problems on staff desktop devices, ICT staff will not be responsible for any loss of data on the device resulting from any action undertaken as part of support work. Users are obliged to have backups of all of their files prior to any troubleshooting being undertaken by ICT staff. However, ICT staff shall be responsible for loss of data negligently or recklessly attributed by them.

8. Internet Services

The use of email and the Internet are efficient and cost-effective ways of communicating and obtaining information. If properly used, such means of communication are valuable business tool. However, improper or inappropriate use of email and the Internet can have an adverse effect on the KCMUCo's business. Such use can also have serious legal consequences and therefore should be highly discouraged.

9. E-mail and Internet Use

1) The following uses of the e-mail and Internet system are considered unacceptable:
   a) Use any E-mail which is not of College's directives for official purpose for example Yahoo, Gmail, Hotmail and so on;
   b) Use of the KCMUCo's system to access, review, upload, download, store, print, post, or distribute pornographic, obscene or sexually explicit material;
   c) Use of the KCMUCo's system for political campaigning;
   d) Use of KCMUCo's system to transmit or receive obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language;
   e) Use of KCMUCo's system to access, review, upload, download, store, print, post, or distribute materials that use language or images that are inappropriate to the work setting or disruptive to the work environment and will not post information or materials that could cause damage or danger of disruption;
   f) The use of KCMUCo's system to access, review, upload, download, store, print, post, or distribute materials that use language or images that advocate violence or discrimination toward other people or that may constitute harassment or discrimination;
   g) The use of the KCMUCo's system knowingly or recklessly post false or defamatory information about a person or organisation, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks;
   h) The use of KCMUCo's system to engage in any illegal act or violate any applicable laws;
   i) The use of the KCMUCo's system to gain unauthorised access to information resources or to access another person's materials, information or files without the implied or direct permission of that person;
   j) The use of the KCMUCo's system to post private information about another person or to post personal contact

information about themselves or other persons including, but not limited to, addresses, telephone numbers, work addresses, identification numbers, account numbers, access codes or passwords, and will not repost a message that was sent to the user privately without permission of the person who sent the message;

k) To attempt to gain unauthorised access to the KCMUCo system or any other system through the KCMUCo system, attempt to log in through another person's account, or use computer accounts, access codes or network identification other than those assigned to the user.

l) The use of the KCMUCo system to violate copyright laws, or usage licensing agreements, or otherwise to use another person's property without the person's prior approval or proper citation, including the downloading or exchanging of pirated software or copying software to or from any KCMUCo computers;

m) The use of the KCMUCo system for unauthorised commercial purposes or for financial gain unrelated to the official business of the KCMUCo. Users shall not also use the KCMUCo system to offer or provide goods or services or for product advertisement, other than for work purposes

n) If a user unintentionally accesses unacceptable materials or an unacceptable Internet site, the user shall immediately disclose the inadvertent access to an appropriate manager. This disclosure may serve as a defence against an allegation that the user has intentionally violated this policy.

1) Authorised Personal Use

a) Users are entitled to make reasonable personal use of email and Internet facilities outside normal working hours. Such use must be consistent with this policy. The KCMUCo reserves the right to discontinue this entitlement for all or some employees if it is of the views that the use of e-mail and Internet facilities as excessive or inappropriate;

b) Users are reminded that any personal use of email cannot be considered private and may be subject to monitoring in

accordance with this policy. Users must make their own arrangements to save electronic or paper copies of their personal emails; the KCMUCo does not accept any responsibility for the safe storage of personal emails, which may be deleted at any time.

c) User who is terminated or resigned his/her e-mail account shall be deleted immediately. If it happens that the user holds passwords for any KCMUCo ICT systems shall be required to hand such passwords to ICT directorate without undue delay.

d) Users are advised to use e-mail applications to avoid not accessing e-mails during network downtime hours. User may consult ICT directorate for such installation.

2) Unauthorised Use

The Computer's system and networks, and provision of email and Internet facilities, must not be used for the creation, transmission, downloading, browsing, viewing, reproduction or accessing of any image, material or other data of any kind which:

a) is illegal, obscene, pornographic, indecent, vulgar or threatening;

b) contains unacceptable content, including but not limited to, sexually explicit messages, images, cartoons, jokes, or unwelcome propositions, or any other content which is designed to cause or likely to cause harassment or provocation of any other person or organisation based on sex, sexual orientation, age, race, national origin, disability, religious or political belief;

c) is defamatory, slanderous or libellous;

d) deliberately introduces viruses into the email or Internet systems of the KCMUCo or any other party or is designed to deliberately corrupt or destroy the data of other users;

e) conflicts with the KCMUCo College's commercial interests;

f) infringes or may infringe the intellectual property or other rights of the KCMUCo or those of a third party;

g) is part of a chain letter, "junk mail" or contains unsolicited commercial or advertising material;
h) violates the privacy of other users;
i) is in breach of the duty of confidentiality which the KCMUCo owes to the Public and KCMUCo Staff;
j) disrupts the work of other users;
k) users shall not send emails which make representations, contractual commitments, or any other form of statement concerning the KCMUCo unless they have specific authority from the KCMUCo administration to do so. Users must not register KCMUCo email addresses on Internet lists or websites inviting downloads, automated email or remote access.

10. Confidentiality

1) All KCMUCo information exchanged by the means of email is subject to confidentiality. No information gained through emails may be disseminated or passed to third parties for whom it was not intended by the originator of the email. If an email is misdirected and you receive an email, which was not intended for you, you must at once notify the originator with information about the circumstances in which you received it. In no circumstances may such an email be forwarded to another, except as part of an investigation into the causes of the misdirection.
2) Emails to recipients external to the KCMUCo shall carry an automatic disclaimer to protect the interests of the originator and of the KCMUCo.
3) Internal emails between two staff members of the KCMUCo shall not carry such a disclaimer. The proper use of internal emails is governed by this Policy. Any improper use of information contained within an internal email shall be considered gross misconduct.

11. Privacy and Monitoring

KCMUCo may undertake the following:

1) Monitor and record any e-mails which are transmitted over its computer system;
2) Monitor or record the use of the Internet by employees, and the nature of material downloaded from the Internet;
3) Monitor or record any use of computer equipment and user sessions
4) To ascertain whether the KCMUCo's practices, policies and procedures have been complied with.
5) To investigate or detect the unauthorised use of the KCMUCo's computer system;
6) To secure the effective operation of the KCMUCo's computer system;
7) To determine whether any communication has been made which relates to the business of the KCMUCo; or
8) For the purpose of preventing or detecting crime; any e-mails sent by employees may therefore be intercepted and monitored by the KCMUCo for any of the above reasons. Accordingly, any messages which are sent are not private. If you wish a message to be confidential, or if you wish any Internet access to be confidential, you should not use the College Computers' system.

12. Access to ICT venues

All ICT related venues should be booked prior to use, information and booking is centralised at ICT office.

13. Access to Server Room

1) The server room is the room which houses the KCMUCo ICT infrastructure. Only Authorised Personnel are allowed to enter. Provost, DPA, DPAA, of the KCMUCo are allowed to enter accompanied by the company of ICT personnel. The server room shall have the CCTV Camera for server room monitoring and system security.

2) All individuals accessing the ICT Server Rooms must sign in and out of the ICT Server Room(s) Access Log. This includes all visitors, who must be accompanied by ICT staff at all times. These log sheets are retained by the Head of ICT.
3) Tailgating other staff in order to enter ICT Server room(s) is not permitted, anyone caught doing that will be given oral warning while repeated offenders will be disciplined accordingly.
4) In Case of emergence, The ICT Personnel in charge shall have access to the server room.

14. Server Machines

1) All software on servers must be authorized and requested by system owners, unauthorized software or data will be removed.
2) Anti-virus software will be installed on every windows server and kept up-to-date.
3) Password on the server machines will be under the custodianship of Directorate of ICT under supervision of DPA. Hence not all personnel will have password access.
4) All servers will sit behind firewalls, which mean access to these servers to the external environment will be by authorization. Any external support that may be required should then be addressed prior to the Director of ICT and the team (If need arise).

15. Environmental Protection

1) All servers will be protected from surges, spikes, sags or brownouts in the electricity supply by the use of Uninterruptible Power Supplies.
2) All servers will be protected from excessively high temperatures and fire by temperature control and fire alarm.
3) Security camera will be installed and controlled so as to increase security within the premises.

16. Network Tools and devices

1) All of the network devices/tools should be configured on the base of preventing/filtering malwares, spywares, worms, and Internet viruses specifically to the firewall that is within our network.
2) All of the network devices/tools password should not be disposed to public except to ICT director, DPA, and IT personnel in charge.
3) Ensures a continuous updating of network devices/tools thus preventing vulnerable loops within the devices/tools.

17. Security Camera

1) Management of Security Camera Systems

The ICT Directorate is responsible for the management of all video surveillance systems used at the College and has exclusive control of the release of video recordings produced by this system. Other departments shall not install video surveillance system without the knowledge and approval of the ICT Directorate.

2) Security Camera Monitoring

The video surveillance systems are capable of being monitored on a continuous basis. The IT personnel in charge will generally view video surveillance cameras on a periodic basis or in response to a specific incident. Because of increased responsibilities of the IT personnel, the video surveillance system is not monitored on a continuous basis.

3) Security Camera Recording

a) All video surveillance cameras are capable of being recorded continuously by a digital video recording system. Recorded video is used exclusively for the investigation of security and safety incidents and not for other purposes.

b) Recorded video is not made directly available to employees, or the general public. In the event that a security incident occurs, employees should report the incident to the KCMUCo management and the management will consult the ICT Directorate for further clarifications and rectification.

c) If the event occurred in an area where video surveillance coverage is available, the ICT personnel in charge together with the ICT Director will review the recorded video and make a determination if any video relevant to the incident is available.

18. Computer, ICT Procurement, Inventory, College Website and ICT Budget

1) Computer Use

a) Computers are an integral part of everyday business life and we cannot escape the continuing growth in their use. This means that the monetary investment by the KCMUCo in infrastructure and IT Personnel is huge to the point where the effect of IT costs cannot be disregarded in the cost budgeting. Misuse of equipment can cause losses to the KCMUCo and cannot be tolerated.

b) Examples of what are not allowed include:

i. Unofficially load any program strictly not authorised and duly licensed for work purposes by the IT Directorate onto any computer. This includes games, screensavers, and unlicensed software's and so on;

ii. Not to stream for entertainment in work time. Sometimes seems to be a feeling amongst people that it is an allowable pastime or of lesser concern. This train of thought should be severely discouraged and the offence be put into perspective;

iii. Not use the KCMUCo system to vandalise, damage or disable the property of another person or organisation, not make deliberate attempts to degrade or disrupt equipment, software or system performance by spreading

computer viruses or by any other means. Also it is strictly prohibited to tamper with, modify or change the KCMUCo system software, hardware or wiring or take any action to violate the KCMUCo security system, and shall not use the KCMUCo system in such a way as to disrupt the use of the system by other users.

2) ICT Procurement.

a) Users shall not use the KCMUCo budget to purchase ICT goods or services for official use without authorisation from the Provost (Accounting Officer), Deputy Provost Administration (DPA), KCMUCo ICT directorate in charge, KCMUCo Tender Board and other relevant organs applicable at KCMUCo.
b) Users planning to request any ICT related hardware/software shall liaise with ICT directorate for verification before submitting requisition to Procurement Management Unit for procurement process.
c) The assessment survey shall be conducted prior the purchase of ICT equipment/infrastructure.
d) The ICT personnel who verify the purchase of the hardware/software which not necessary or not relate with user's duties. For example, verifying the purchase of ICT hardware/software of high capacity and therefore leading to high cost not necessarily required by the user in day to day activities shall be held accountable.
e) College shall not bear cost associated with any requisition of ICT hardware/software which is not channelled through College procurement system or which is outside of user budget of the respective year unless authorized by the accounting officer in extenuating circumstances.

3) Inventory

a) All ICT related hardware/software are required to enter into KCMUCo ICT inventory within 3 days once purchased. The ICT

inventory is kept by the ICT Directorate, Accounts, and procurement. The Deputy Provost Administration may require the ICT inventory report at any time as shall be deemed necessary and equitable.

b) ICT Directorate shall from time to time updates DPA regarding the status of the College ICT assets as shall be deemed feasible.

4) College Website

KCMUCo has full right for its website; ICT staff in charge should be allowed to update the website from time to time with prior permission from DPA.

19. ICT Directorate

It is hereby established the directorate of ICT which shall be headed by the Director accountable to Deputy Provost for Administration. The directorate is hereby empowered to generate incomes as shall be deemed necessary.

1) Role of the Directorate.

a) Administration

i. The directorate through Director shall be responsible to oversee all activities of the directorate staff members by assigning tasks and area of supervision so as to increase accountability, effectiveness and efficiency.
ii. The directorate shall take charge of the safety of the ICT facilities such as computer lab, e-library, and server rooms and ensure users adherence with this policy.
iii. Moreover, it is with great interest for the directory to create strong team with creative mind that shall foster innovative ideal, for this reason directorate identify, acknowledge and establish rewarding system.

iv. The directorate will provide one hub for all other entities to officially request the service this including Internet distribution.

b) Coordinating

i. Resources are scarce with alternate use; hence directorate shall take charge in ensuring that all resources available are utilized in the effective and efficient manner that will be for the best interest of the KCMUCo development.

c) Resources referred here includes to the following:

i. Computing devices**;**
ii. Printing devices;
iii. Projectors and Public Announcements systems;
iv. Security Cameras;
v. LAN resources;
vi. AMIS;
vii. LCMS+;
viii. Moodle;
ix. Inventory;
x. D-Space;
xi. WAN resources;
xii. MOOC;
xiii. Mentor IRB;
xiv. CITI;
xv. E-library;
xvi. Video Teleconference.

d) Planning and design

i. With growing of the College it's inevitable for the directorate to forecast activities, demands and design way forward that will serve as framework.

ii. More over it is role of the directorate to provide College with mile stone/checkpoint and work-plan clearly showing how those plans can be achieved.

e) Development and Training

Directorate shall oversee trainings required for capacity building as well as uses its members to offer training to the end users such as students and staff according to the planning addressed in the directorate.

Henceforth this will include the following aspects:

i. Workshops
ii. Seminars
iii. Short courses

Directorate shall prepare a framework that will answer the question on what, when, who, and how the above aspects of the development will be handled without bias and disruption of the daily routines.

f) Advice and consultation

The directorate shall stand as internal professional advisory body in matters relating to the technologies in the KCMUCo administrative organs.

g) Liaison Manager

The Directorate shall act as interface between ICT team, resources and services available to the potential clients including existing projects, newfound projects at KCMUCo and KCMC campus in general.

h) Objective of the Directorate.

i. Increase effectiveness in the general ICT services

ii. Load balancing job assignment/rotation integrating ICT staffs to understands College logic model and strategic plan.
iii. Define communication channel-there should be proper line of communication between staff within directorate and all other departments that will be working together.
iv. Raise awareness- The directorate will ensure other users within KCMUCo understands its existence as well as its functionality.
v. Link between management- the objective of directorate is to lower gap between management governing body and the ICT mission. It's of the great interest for ICT directorate to move in the same direction as College vision.
vi. Safeguard interest of College as well as members. It's crucial for ICT to provide best service that will serve purpose for staff that will be using in conjunction with students

h) ICT Directorate Budget

i. The ICT Directorate, in collaboration with other College Directorates /Departments shall actively participate in determining their Budgets and shall always operate within the Budget approved by College Governing Board. Any reallocation or expenditure beyond budget shall require written authorization from accounting officer;
ii. All IT procurements shall be endorsed by the head of ICT Directorate. The IT requisition may be initiated by any other department but ICT expert shall determine what is the right hardware or software needed for the department.

20. Liability

Any criminal liability accruing in relation with this policy shall be criminally handled. Students or class which shall damage/lost College ICT facilities shall be required to pay forthwith. The College may take any other measures as per existing Labour laws.

21. Right to privacy

a) Users should understand that all equipments, as well as the information it contains, belongs to the KCMUCo. Users should consequently have no expectation of privacy related to the use of any KCMUCo system.

b) KCMUCo has the fullest right to monitor the email and Internet system, as well as accessing data such as emails received by employees. In the spirit of mutual respect and trust employees must also be aware that it is not the policy of the KCMUCo to monitor the email on a constant basis, and that they will be notified if specific departments will be under constant monitoring for certain reasons. Routine maintenance and monitoring of the network might however reveal that violations of the policy by specific users have occurred, which may result in an individual investigation, without any advance warning.

22. Private use

1) The KCMUCo agrees that a certain amount of incidental private use is allowed. This use however must not exceed what would be regarded by any reasonable person as fair and just, and is subject to the terms and conditions of the policy.

2) Private use of the system is a privilege and not a right, and what would be considered suitable use on a private account on another system will not necessarily be suitable for the KCMUCo system. The KCMUCo may restrict the users' access to the system at management's discretion.

23. Failure to comply with the Policy

1. Any failure on the part of an employee of the KCMUCo to act in accordance with the Policy may result in disciplinary action being taken against him or her depending upon the severity of the breach of the Policy
3) Any failure to comply with the Policy on the part of a User who is not an employee may result in the immediate termination of the contractual or other relationship between that person or organisation and the College. The non compliance attributed by KCMUCo employee shall be handled in accordance with National and College legal framework.
4) Any unauthorised use of file(s), application(s), email(s) or the Internet by a user at KCMUCo shall be immediately reported to the respective authority.

24. Review of ICT Policy

This policy shall be reviewed on regular basis to accommodate demands arising from advancement in science and technology. Under normal circumstances the policy will be reviewed every three years. However, nothing shall limit the College top management inherent power to review this policy at any time as shall be deemed to be necessary and equitable.

25. Interpretation & Approval

This policy shall be interpreted and applied together with other ICT relevant national legal instruments and college policies.

When this policy conflict with ICT related national laws the later shall prevail. However, when this policy conflict with other college policy in ICT related matters this policy shall prevail.

This policy come into force after being approved by the College Governing Board in its 27th meeting held on 29th April 2016.

26. References

Kibabii University College (A constituent College of Masinde University of Science and Technology), Information and Communication Technology (ICT) Policy, June, 2014.

Masinde Muliro University of Science and Technology, ICT policy 2012.

Millennium Development Goals (MIDGs).

Muhimbili University of Health and Allied Sciences, Information & Communication Technology (ICT) Policy and Procedures, 2014.

Sokoine University of Agriculture, Information and Communication Technology Policy, 2nd Edition, as approved by SUA 133rd Meeting of the Council held on 27th March 2014.

The Nelson Mandela African Institution of Science and Technology (NM-AIST), ICT policy, February 2011.

The United Republic of Tanzania, Ministry of Communications and Transport, National Information and Communications Technologies Policy, March 2003.

The University College of Cape Coast ICT Policy, 2004.

The University of Sydney, Policy on the use of University information and communication technology resources (ICT resources).

University College of New South Whales (UNSW) Website policy 2004 Vision 2030, 2007.