KAIMOSI FRIENDS UNIVERSITY COLLEGE

(A constituent College of Masinde Muliro University of Science and Technology)

ICT POLICY IMPLEMENTATION GUIDELINES

JULY 2017

www.kafuco.ac.ke

DOCUMENT CONTROL

Title	Reference	Status	Date
ICT POLICY IMPLEMENTATION GUIDELINES	Version 0	Developed in Principal Division	21st February, 2017
Draft 1	Version 1	Circulated to Management and comments incorporated	16th May, 2017
Revised Draft 1	Version 1	Adopted by Strategic Planning & Development Committee	15th July, 2017
Final Approved	Version 1	Approved by the Council	16th July, 2017

Table of Contents

ANNEX 1: HARDWARE GUIDELINES

1.1 The hardware components cover:

a) Computers: Servers, desktop computers, portable computers (laptops, notebooks), etc.
b) Output, input and storage equipment: Disk storage systems, printers, scanners, L.C.D Projectors, Removable media, Photocopiers etc.
c) Networking equipment: Routers, switches, modems, etc.
d) Communication systems: Very Small Aperture Terminal (VSAT), Fiber backbone, cabling systems, etc.
e) Other ICT accessories: Digital, Camera / Cam coders, Power Backup Equipment (UPS)

The following guidelines are aimed at ensuring that the ICT systems are protected from:

a) Unfavourable environmental conditions.
b) Unauthorised access.
c) Malicious attacks (virus, worms, Trojan horses, etc.).
d) Inappropriate handling by IT personnel and users.

1.2 Environmental Conditions

The policy guidelines on environmental conditions are aimed at ensuring that the environment within which the ICT systems operate is protected against inappropriate levels of power, temperature, humidity, and also against fire and dirt. Consequently, the following are to be noted:

1.3 Power

Power supply to computers and accessory equipment shall be clean, safe and uninterruptible. This will involve the provision of:

a) Standby generators/battery banks, especially for centralised systems.
b) Uninterruptible Power Supply (UPS).
c) Stabilisers.
d) Power protection devices against surges and lightning strikes.

1.4 Air Conditioning

The server room and computer labs shall have air conditioning systems that operate at all times. The air conditioning systems shall keep the room within the equipment manufacturers' recommended specifications for temperature and humidity throughout the year.

1.5 Lighting

Adequate lighting shall be provided in the server room and computer labs.

1.6 Fire

a) Computer labs and server rooms shall be protected by smoke detectors and fire alarm systems.
b) Fire extinguisher(s) shall be provided for computer labs and server rooms. They shall be periodically tested to ensure that they are in good working condition.
c) IT personnel in charge shall periodically be made to undergo fire prevention drills.

1.7 Cleaning

a) The server room, computer labs and computers shall at all times be kept clean of dust, dirt and rubbish.
b) Eating and drinking shall be prohibited at the computer labs and server rooms.
c) The computers shall be kept clean and free from contamination.

1.8 Asset Management

a) User Departments shall track their computer systems through the use of an Asset Register. The Asset Register may be a computer program, notebook but preferably a spreadsheet with the following basic information: Type of Equipment, Serial Number, Model, Specification, Date Purchased, Location (Room, Office), Cost, Life-Cycle (In Years), Status (in operation, faulty or under repairs).
b) The ICT Directorate shall provide a template for the Asset Register and make it available to user departments through the website.
c) Asset Identification: All IT equipment shall be identified by an Asset Number in line with the University College’s asset naming and identification scheme.

1.9 Tracking movement of equipment

a) An equipment movement log book shall be maintained to track movement of ICT equipment. Details shall include equipment specifications, name of user, where the equipment is being moved from and to, why it is being moved and the date of removal and replacement. A template shall be provided by the ICT Directorate through the website.
b) Any IT equipment other than the individual’s laptop taken off site shall have the supervisor or IT Officer in charge authorisation for removal. Failure to comply with this directive shall result in disciplinary actions against the person. The person shall be held liable for any damage to equipment or loss of equipment.
c) Removal of any IT equipment other than laptops from its normal place of use, *e.g.* from one computer lab to the other for any reason, shall be authorised by the IT Officer in charge and logged in the equipment movement log book.
d) Unauthorized removal of any IT equipment from its normal place of use without permission by any person shall attract sanctions including

withdrawal of access privileges, payment for loss or damage to ICT facilities and suspension or expulsion from the University College. The University College also reserves the right to report any illegal activities to the appropriate legal authorities, *e.g.* the Police.

e) Lost or stolen ICT equipment shall be reported to the appropriate Head of Department and the Chief Security Officer.

f) Costs/charges due to damage or otherwise as a result of negligence on the part of users shall be borne by the user in question.

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

h) Cabling shall be kept tidy and neatly arranged to prevent any work hazards. Cabinets for devices shall be used where possible. Cables shall also be terminated in all cabinets and labelled for easy identification.

1.10 Troubleshooting, Repairs and Maintenance

i. There shall be established an ICT Section referred to as “repairs and maintenance”

ii. Desktop computers, Portables (laptops, notebooks, and Personal Digital Assistants (PDAs)) and Printers that develop faults shall be sent to the ICT Directorate for repairs and maintenance.

iii. IT personnel shall document and keep system settings and drawings up to-date.

iv. The University College shall contract an external ICT service provider to maintain such hardware equipment. User Departments shall liaise with the ICT Directorate to conclude maintenance agreements with external ICT Service Providers.

v. The ICT Directorate shall provide templates for maintenance contracts and make them available to user departments through the website.

1.11 Disaster Recovery and Contingencies

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

1.12 Other User Responsibilities

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

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

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

iv. Only the University College staff and students are allowed to use the University College's ICT facilities. Visitors and guests shall obtain authorisation from the IT Officer in charge before use.

v. Unauthorised or improper use of the University College's ICT facilities and equipment by any person shall attract sanctions against the person. The sanctions shall include withdrawal of access privileges, payment for loss or damage to ICT facilities and suspension or expulsion from the University College. The University College also reserves the right to report any illegal activities to the appropriate legal authorities, *e.g.* the Police.

ANNEX 2: SOFTWARE GUIDELINES

Software shall include but are not limited to: Network Operating Systems, PC Operating Systems, Application Software, Antivirus Software, In-house developed Systems and off-the- shelf Systems.

Most of the software supplied to Users through the University College is licensed for Educational Use only. Those Users wishing to use software or systems for consultancy or commercial activity should ensure that either the University College licenses permit this type of activity or that they arrange to licence a copy/copies of the appropriate software specifically for the activities concerned. If in doubt, users should consult the IT Helpdesk.

Software installed on all administration machines shall be as the standards provided by the ICT Authority from time to time. The following shall govern the appropriate use of software:

i. The University College shall maintain a record of software available centrally for use in the University College together with details of licensing arrangements. (Records of centrally licensed software are maintained by ICT Directorate, whilst Schools and Departments are responsible for maintaining lists of software currently held and for establishing the legality of all their holdings.)

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

iii. Copying of Software: Users shall not allow KAFUCO licensed software and/or associated documentation to be copied by outsiders and shall not themselves make copies other than those provided for in the relevant licensing agreements. Appropriate disciplinary action including criminal penalties shall be prescribed by the University College Management for the breach of this directive.

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

v. Faculty/Department/Centre Software Applications: In order to benefit from volume discounts and common installation and setups, the ICT Directorate shall coordinate the procurement and implementation of common software applications used by the academic units. Such software applications shall be run at the faculty/department level where it is used.

vi. Software Configurations: Software configurations shall be documented for easier reference.

Note: a person who breaches this Policy guideline faces disciplinary action including withdrawal of access privileges, payment for loss or damage to ICT facilities and suspension or expulsion from the University College. The University College also reserves the right to report any illegal activities to the appropriate legal authorities, e.g., the Police.

2.1 Antivirus

i. All computers in the University College shall have the standard antivirus software of the type Kaspersky installed.
ii. The ICT Directorate shall ensure that the relevant Antivirus is installed on all computers once notified. It is the responsibility of every user to avail their machines for the installation of the antivirus software.
iii. The ICT Directorate shall provide automatic updates of the antivirus through the network for computers connected to the network once a first-time installation is done.
iv. For computers not connected to the network, the officer in charge at the Department shall liaise with the ICT Directorate to have the updates done regularly.
v. Any software or data received from any external source, including the original manufacturer and the Internet, shall be treated as suspect and not installed, executed or used in any other fashion until it has been scanned for viruses using the University College's standard virus detection software.
vi. Users shall call the attention of the Departmental IT personnel immediately for assistance if a virus incident or activity is noticed and cannot be cleaned by the user. The problem shall be reported to the ICT Help Desk if problem persists.

2.2 Integrated Management Information Systems

The University College shall systematically implement information systems that are seamlessly integrated to ensure effective service delivery, sharing of information, decision making and reporting. This shall be achieved through:

a) Implementation of enterprise resource planning systems covering:
   i. Financial management
   ii. Academic Management including students records management
   iii. Human Resource Management
   iv. Inventory and procurement management
   v. Asset Management
   vi. Health and medical records management
   vii. Library and e repository management
   viii. Document Management system
   ix. Student and Staff portal services
   x. Security Management
b) Implement effective email management systems
c) Implement help desk management system to facilitate effective user support operations
d) Review and enhance electronic system to manage the documentation of the University Quality Management System (QMS)

The ICT directorate shall be responsible for the maintenance and support of the University College Integrated Management Information Systems.

ANNEX 3: NETWORK GUIDELINES

The University College network shall comprise optical, wired and wireless connections throughout the various college sites. Only contractors engaged by the IT department and the members of the IT department shall have direct access to any hardware component of the network, and interfering with any part of the wiring, optical fibres and hardware by any University College member will be deemed to be a serious matter.

3.1 Management of Network Configuration

The configuration of critical routers, firewalls and other network security devices will be the responsibility of the ICT directorate who will maintain and secure the devices. No IT equipment may be connected to the College network without approval by ICT directorate. The ICT directorate also reserves the right to disconnect and remove equipment that has not been properly approved.

3.2 Connecting to the ICT Network

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

1) Users of portable computer devices who wish to directly connect to the University College network are required to register their computer with the ICT Directorate.
2) 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.
3) No computing device may be directly connected to the University College network while at the same time connected to external network.
4) All connections to the University College's ICT networks must conform to University Internet Protocol (IP) addresses.
5) Configuration of personal computers, printers, *etc.,* for network access shall be done by the ICT Directorate.
6) Any computing device that is connected to the University College network shall be properly protected against hacking, viruses and similar security threats, through appropriate use of security technology, including anti-virus software. The University College network infrastructure shall be secured against:
    a) Email Spam: These are unsolicited Emails that users receive through the Internet.
    b) Intruder or Hacker Break-ins: The University College's network like all networks connected to the Internet is susceptible to attacks or intrusion by eternal users.
    c) Virus, worms, spyware which create various dysfunctions in computer systems.

7) To avoid interoperability or poor network connectivity problems, User Departments are advised to contact the ICT Directorate before installing or making any changes in their Local Area Networks (LANs) as well as workstations.
8) Users or User Departments shall seek clearance from the ICT Directorate for any third-party network connections to the Internet or any external networks.

3.3 Use of the Network

1) The University College 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 College 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.

3.4 Firewall

The University College network incorporates a firewall to control data traffic into and out of our local network; this increases the security of our network and helps to keep the threat of malicious attacks to a minimum and to keep confidential information secure.

All internet access from the University's network must pass over the situated firewall. The default configuration, unless otherwise specified, is that services are forbidden. All users are allowed to exchange emails in and out through the firewall.

Detailed logs shall be kept (where possible on a separate server). They shall be automatically analysed, with critical errors generating alarms. Logs shall be archived for at least six months and up to one year. The non-trivial log entries should be examined daily.

3.5 External Access to University ICT Network

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

3.6 Domain Name Services

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

ANNEX 4: ICT SECURITY GUIDELINES

The responsibility for protecting ICT systems and information rests with all staff, students and third parties who use or have involvement with the systems. Both the University College ICT user community and ICT Directorate have responsibilities to ensure compliance with this Policy in order to ensure that:

a) The *integrity* of information is maintained, so that it is accurate, up to date and fit for purpose;
b) Information is always *available* to those who need it and there is no disruption to the business of the University College;
c) *Confidentiality* is not breached, so that information is accessed only by those authorised to do so;
d) The University College meets its legal and statutory requirements;
e) appropriate controls are in place so that Users have access to accurate, relevant and timely Information but that Users of KAFUCO ICT resources do not adversely affect other Users or other Systems; and
f) The reputation of the University College is safeguarded.

The end-to-end information security management process will operate at an optimal level where education and awareness of each other's responsibilities in the end-to-end process and commitment to individual responsibilities is high.

4.1 Access Control

The University College at a minimum will ensure:

a) Authentication requirements, including on-line transactions and services must be appropriate for the security classification of the Information;
b) Access to the University College network and Information Systems requires specific authorisation and each User must be assigned an individually unique personal identification code and secure means of authentication;
c) Policies and/or procedures for user registration, authentication management, access rights and privileges are defined, documented and implemented for all ICT Assets;
d) restricted access and authorised use only warnings must be displayed upon access to all Systems which have this capability.

4.2 Physical Access and Systems Controls

a) Access to Information Systems at the University is to be provided to University College Clients for the purpose of carrying out work, study or other activities as agreed with the University College and as appropriate to the client's role. Unattended access equipment (e.g. PC) is to be protected through physical or electronic means (e.g. System timeout).
b) Physical access controls for the University College premises will be implemented in accordance with the risk and the importance of the Information Asset to be protected.

c) Security risks shall be assessed and managed in relation to the physical location of an Information Asset, particularly where this location is offsite from University College premises.

d) Appropriate control mechanisms (e.g. Username and password) will be in place for authenticating access to all non-Public Information Systems and Information Assets. Access control must be in accordance with the Information Classification.

e) Access granted to Third Party University College Clients is to take into account the risks involved, with adequate controls put in place to protect the University College's Information Assets (e.g. the most limited access rights in the system as possible in order to carry out the work). In addition the University College may require Third Party University College Clients to sign a University College confidentiality agreement.

f) In assessing risks to Information Systems, the user must consider the security of the information in all media formats that will be used (e.g. hardcopy). Furthermore, consideration is required when information may be stored on mobile equipment which can be transported offsite (such as laptops, USB sticks and mobile phones).

g) Remote access to Restricted Information Systems will only be provided by the ICT Directorate with the explicit authorisation of the head of the user department.

h) Ownership of information, data and software within the University is assigned in a manner consistent with the University College's Intellectual Property – Governing Policy or with other contracts and agreements.

4.3 Server Room and Computer Laboratories

a) Server room and computer labs shall be adequately secured at the doors and windows with locks and burglar proofs.

b) A logbook or electronic system shall be maintained at the sever room to record entries and departures by IT personnel, visitors and service providers. Details of date, time, personnel/student/staff, purpose, and exit time shall be recorded in the logbook.

c) Provision (eg, pigeon holes) shall be made for safe keeping of student bags in the computer labs; bags shall not be allowed into the computer labs.

d) All students who use the computer labs shall be duly authorised through a registration process.

e) At the end of each day of work, Lab Technicians or IT personnel in charge shall check all equipment to ensure that they are intact and in good operating condition.

f) A log book shall be maintained to record incidents, events and problems at the computer labs.

g) Anyone in possession of the keys to the server room or computer labs is totally responsible for that key. His/her responsibilities shall include not handing over the key to anyone else while the key is signed out to them and not making duplicates of the key.

h) Any irresponsibility on the part of anyone in possession of the keys to the server room or computer labs that results in loss of any item or improper use of the facilities shall attract sanctions such as prohibition to use the facilities and payment for the loss of any item.

4.4 Logical Control (User IDs and Passwords)

4.4.1 Username and Password Control

Primary access to all the College IT facilities is governed by a network username and password giving access to a set of network services, depending on department and status. The ICT directorate maintains procedures for the issue of and closure of network accounts. Authorisation of access to systems and to the data held by them is the responsibility of both the system owner and ICT directorate. The University College aims to minimise the number of accounts required by each individual.

The control of network passwords is the responsibility of the ICT directorate. Re-issue of network passwords is through the ICT directorate. System administrator passwords will be issued on the express authority of the ICT Director on a need-to-know basis. Such passwords will be changed regularly and when authorised system administrator staff leave. The ICT directorate must be notified by department heads when staff leave and will be responsible for removing their network accounts.

Responsibility for retention of any files held by staff that leave lies with their department and should form part of their staff exit procedure. Departments responsible for electronic information assets will be informed when staff authorised to access those assets leave and will be responsible for controlling access rights to those assets.

a) Generally all users of computing and networking facilities shall be authorised through the assignment of User IDs and Passwords.
b) All guests and visitors to the University College shall sign-up for Guest User Accounts. The essential 'dos and don'ts' shall be explained to such visitors and guests, prior to their use of the University College’s computer facilities.
c) Users are advised not to disclose their personal passwords to anybody. Users are responsible for protecting their personal password and for the consequences of their password being known by others.
d) Users shall not sign on to any University College system using a User ID other than that assigned to them.
e) Users are accountable for all system activities that occur using their User ID and password.
f) Initially assigned passwords for any users shall be changed upon first login.
g) Good practice with passwords shall largely be enforced by the system settings. However, users are advised to follow these guidelines:
    i. Passwords shall be a minimum of eight characters in length and they shall either contain both alphabetic and numeric characters or be a phrase of two or more unrelated words.
    ii. If Password change is prompted by the system, please do so when requested to.

iii. Passwords shall be changed immediately if the user believes he or she has been compromised or noticed anything unusual.
iv. The standard password protected screen saver shall be activated when the PC is left unattended.
v. Users shall log off when leaving their personal computers for a period of 30 minutes or more.
vi. The PC shall always be logged off and switched off before being left overnight unless it is running an overnight process, in which case the screen saver shall be activated.

4.5 Two Factor Authentication

Two-factor authentication (e.g. smartcards or biometric devices, such as fingerprint recognition) shall be applied to users with access to critical business applications or sensitive information and to users with special access privileges or access capabilities from external locations.

4.6 Security Breaches

Any suspicion of breach of the policy must be reported to the ICT Help Desk or a line manager immediately. Failure to do so constitutes a breach of this policy. The line manager should then report the issue to the Service Desk or direct to the ICT Director. The ICT Director has the power to authorise ICT support staff to suspend access to all accounts affected by the breach. This may include accounts controlled by other departments. Suspensions will be lifted in three working days unless further suspension is authorised by the Principal.

In cases where investigation of traffic or content of user accounts is necessary then ICT technical staff will carry out such work under direct instruction from the ICT Director following authorisation from the Principal. The University College will involve the Police in all cases where they believe illegal activity may have taken place

ANNEX 5: INTERNET GUIDELINES

The Internet facility is primarily provided to enhance learning, teaching, research and administrative functions of the University College. The Internet complements the University College library for researching materials and ideas from a variety of sources both national and international. The facility shall not be used to download personal collection of music, movies or pirated software. Any person that uses the Internet to download personal collections of music, movies or pirated software shall be liable to disciplinary action including withdrawal of access privileges, payment for loss or damage to ICT facilities and suspension or expulsion from the University College. The University College also reserves the right to report any illegal activities to the appropriate legal authorities, e.g., the Police.

The University College is aware of the growing use of mobile equipment and is expanding its Wi-Fi provision accordingly for all members of the University College. The University College shall provide a wireless system that delivers a wireless service to both staff and students managed by the ICT Directorate. Designated Wi-Fi areas in the University College shall be established.

The wireless network infrastructure shall comprise 3 separate secure WLANs:

1) Staff
2) Students
3) Guests

The staff WLAN shall be available to University college staff using authorized university college equipment only. The student WLAN shall be available to students who have a bona fide University College network account. Wireless access to the Internet for guests, visitors and conference delegates at the main Campus shall be provided on request and necessary approval.

5.1 Monitoring and Control

i. Since the Internet is an unregulated medium it is highly subject to abuse. The ICT Directorate shall regularly inspect Internet files held on computers connected to the University College network, to ensure users have not accessed inappropriate sites or sites that have been expressly forbidden.
ii. Inappropriate sites will be filtered or blocked to ensure that users do not access their materials. Inappropriate sites are those with materials relating to pornography, offensive on grounds including but not limited to ethnic origin, religion, politics and gender.
iii. Any user who finds a possible abuse as well as security lapse on any system shall report the event to the ICT Directorate.
iv. Users who deliberately access inappropriate material or send inappropriate messages to others shall also have their Internet access withdrawn and shall be dealt with in accordance with University College disciplinary procedures.

Misuse of the Internet facility by users who deliberately access inappropriate material or send inappropriate messages to others shall result in disciplinary action, including written warnings, withdrawal of access privileges and suspension or expulsion from the University College. The University College also reserves the right to report any illegal activities to the appropriate authorities, e.g., the Police.

5.2 Disclaimer of Liability for Use of the Internet

i. The University College is not responsible for material viewed or downloaded by users from the Internet.
ii. Users are cautioned that some materials from the Internet could be offensive and inappropriate.
iii. In general, it is difficult to avoid contact with these undesirable materials while using the Internet. Users accessing the Internet do so at their own risk.
iv. Users are to note that Internet traffic can be monitored and traced to the individual user.
v. Discretion and professional conduct is expected.

5.3 Downloading

i. Information that is downloaded from the Internet shall be used for official or academic purposes. Copyright laws shall be respected and the appropriate credit given to the author or source of the information.
ii. The downloading of text or images which contain material of an offensive, indecent or obscene nature is prohibited.
iii. Any software or files downloaded via the Internet onto the University College computers shall be used only in ways that are consistent with their licenses or copyrights.
iv. No user shall use the University College facilities knowingly to download or distribute illegal software or material.
v. No user shall use the University College's Internet services to propagate deliberately any virus.

Any breach of these directives shall result in disciplinary action, including written warnings, withdrawal of access privileges to the Internet facility and suspension. Also individual persons shall be held liable for any infringement of copyright laws as a result of downloaded information from the Internet or distribution of illegal software or material.

5.4 Uploading

Staff must ensure that all information published on intranets/internet does not contain information that is likely to compromise a student or member of staff. All members of staff need to be aware of the possible misuses of online access and their responsibilities towards students. Wherever possible the University College shall use firewall software to ensure that undesirable material is unavailable to the user community.

5.5 Peer-to-Peer (P2P)

i. Use of P2P applications (bittorent) for file sharing and entertainment is deemed to be inappropriate use and shall not be permitted.

ii. P2P usage enable sharing and distribution of copyrighted works, and the Copyright Act makes it illegal to make or distribute copyright materials without proper authorization from the copyright owner. The University College shall enforce protocol or port level restrictions to prevent P2P activities.

iii. Individual persons shall be held liable for any infringement of copyright laws as a result of sharing and distribution of copyrighted works without proper authorisation from the copyright owner.

5.6 E-Commerce

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

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

iii. Inappropriate use of the University College Internet facility to conduct business or e-commerce activities not related to the University College shall result in:

a) Loss of access privilege to the Internet facility and the University College reserves the right to surcharge the person for the use of the University College Internet facility to conduct business.

b) Individual liability to any offence committed as a result of using the University College Internet facility to engage in any illegal activities such as hacking, accessing unauthorized information within and outside the University College or stealing and using of credit cards.

5.7 Chat and Newsgroups

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

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

ANNEX 6: EMAIL GUIDELINES

The Email facility has been provided to enhance the business of the University College through easier, faster communications and interaction among the user community. This Policy provides guidance to users to use the facility in an appropriate and beneficial manner. Official communication should be done through the official University College email address.

6.1 Subscription to Email Facility

6.1.1 Subscription by Staff

i. All staff of the University College are entitled to an Email account.
ii. An Email address shall be created for staff within 2 days, on applying to the ICT Directorate.
iii. Staff shall apply by calling the Help Desk or filling in Technical services request form/system access form addressed to the ICT Directorate. The details required for the Email address are: Name, PF Number, Department and Contact Phone.
iv. Applicant will be required to change the assigned password on his/her first login.

6.1.2 Subscription by Student

i. Email addresses shall be created for students when they register to use the University College Computing facilities and services.
ii. Alternatively, students shall apply for Email address through their respective Departments or by contacting ICT Directorate

6.2 Closure of Email Account

6.2.1 Closure of Staff Email Account

i. The office of the Registrar shall notify the ICT Directorate when a member of staff leaves the services of the University College.
ii. The ICT Directorate shall disable the staff account/Email address. But before this is done, the ICT Directorate shall confirm that all official documents and correspondences received through the mailbox of the staff have been printed and filed by the user departments.
iii. The staff account/Email address shall be deleted three months after the member of staff has left the services of the University College.

6.2.2 Closure of Student Email Account

i. Email accounts of all final year students shall automatically be deleted one month after completion of programme.
ii. Students requiring more than one-month retention of Email account after completion of programme shall submit request through their Head of Department.

6.3 Email Address Naming Convention and Account Types

6.2.1 Naming Convention

The University College's Email address convention is:

i. Individual Email Address: Initial(s)surname@kafuco.ac.ke
Example 1: kotieono@kafuco.ac.ke (Kevin Otieno).
Example 2: dmm@kafuco.ac.ke (David Mumo Maina).
Where there are duplicate Email address names, sequential names shall be used to differentiate the Email addresses:-
Example: kevin.otieno@kafuco.ac.ke;

ii. Departmental Email Address: deptname@kafuco.ac.ke
Example: procurement@kafuco.ac.ke (Procurement Department)
Example2: sci@kafuco.ac.ke (School of Computing and Informatics)
Example3: computing@kafuco.ac.ke (Computing Department)

6.3.2 Sub Domain Email Accounts

Schools and Departments shall request for a sub domain to be created by applying to the ICT Directorate. An Email address with a sub domain will look like: Initiallastname@subdomainName.kafuco.ac.ke Example: pmuindi@finance.kafuco.ac.ke (Finance Department).

6.3.3 School/Unit/Section/Department/Special Purpose Email Accounts

Schools, Departments, Units, Sections or groups shall apply to create a School/Departmental/Unit/Section/Group Email account to send, receive and store official Emails. Special Email accounts could be setup for a specific purpose. Example: registrar@kafuco.ac.ke or research@kafuco.ac.ke

6.4 Security and Confidentiality

a) The University College does not guarantee the confidentiality of electronic mail since it could be intercepted within or outside the University College network.

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

6.5 Legal Implications

Users are to note that Email has the same standing in law as any other document and that insulting someone in an Email shall be considered defamatory and may leave the University College and/or the individual user open to legal action.

6.6 Email Disclaimer

Users shall not transmit personal opinions as those of Kaimosi Friends University College. The following disclaimer will automatically be included as a suffix to all Email messages to addresses external to KAFUCO.

DISCLAIMER: All the information contained in this email message is strictly confidential and may be legally privileged. Such information is intended exclusively for the use of the designated recipient(s). Any disclosure, copying or distribution of all or part of the information contained herein or other use of or the taking of any action in reliance upon this information by third parties is prohibited and may be unlawful. Kindly note that unless expressly stated, any views or opinions presented in this email are solely those of the author and do not necessarily represent those of Kaimosi Friends University College. The recipient should check this email and any attachments for the presence of viruses. If you have received this email message in error please delete it immediately and notify the university through email at info@kafuco.ac.ke

6.7 Leave, Vacation and Travel

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

i. For staff about to take leave, vacation or travel, the Email shall be set to automatically inform senders of their out-of-office status, with an advice to send the message to an alternative Email address if it is official.
ii. Staff travelling outside or within the country, have the option of setting the Email to forward mail messages to an alternative Email system where it would be easier to retrieve.

6.8 Email Data Backup and Storage Management

i. It is the responsibility of the user to backup mails already received in their mailboxes. The central storage Email system shall hold pending Emails for users till they are retrieved by users.
ii. The following guidelines are recommended for managing Emails:
    a) Save your mails as files on your disk regularly and delete from mail box.
    b) Use departmental mailboxes to store official Emails
    c) Adopt the practice of sending copies of official Emails to the departmental mailboxes. Such mailboxes shall be backed up periodically. Occasionally, depending on storage, print Email and then purge.

6.9 Sending and Receiving Emails

i. Responsibility: Users are responsible for Emails they send and for contacts made.
ii. Composing: Email shall be written carefully and politely. As messages may be forwarded, Email is best regarded as public property.

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

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

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

vi. The following are forbidden:

a) Sending of unsolicited bulk mail messages of personal nature.
b) Anonymous messages and chain letters should not be sent.
c) Advertising of personal items.
d) Transmitting any material either as the message or as attachments to a message that is unlawful, obscene, malicious, threatening, abusive, libellous, or hateful, or encourages conduct that would constitute a criminal act or give rise to civil liability or unrest or a breach of the University College's policies. Among those which are considered offensive are any messages which contain sexual implications, racial slurs, gender specific comments, defamatory statements or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability.
e) Users are not authorised to retrieve or read any Email messages that are not addressed to them. Employee shall not use any password or code, access a file, or retrieve any stored information, unless authorised to do so.

A breach of overuse of megabytes and any aspect of this directive on sending and receiving Emails shall result in: disciplinary action including withdrawal of access privileges, payment for loss or damage to ICT facility and suspension or expulsion from the University College. The University College also reserves the right to report any illegal activities to the appropriate legal authorities, e.g., the Police.

6.10 Types of Mailing Lists

Mailing lists shall be created to facilitate communications and dissemination of information in the University College. A mailing list may be moderated or non-moderated. When a list is moderated, messages sent to the list shall first be checked by a moderator before it is released to the list members. For a non-moderated list, messages are sent to the list members without any checks by someone. For the purpose of this Policy mailing lists are categorised into two types: - KAFUCO Staff and Student Mailing Lists; and Other Mailing Lists.

6.10.1 KAFUCO Staff and Student Mailing Lists

a) The KAFUCO Staff Mailing List shall be created and used for disseminating University College-wide announcements, events and news.
b) The list shall be restricted to staff of the University College.
c) All subscribers to the University College Email system are automatic members of the list.
d) The List shall be moderated by the Webmaster/system administrator.
e) The Webmaster is mandated to reject messages sent to the list for circulation based on the following grounds:
   i. When message is of personal nature.
   ii. When message is defamatory or insulting.

6.10.2 Other Mailing Lists

Based on requests from users, the ICT Directorate shall create on the Email server, other mailing lists for Schools/Faculties, Departments or groups that have some common interest or subject matter to share. For instance, a mailing list could be created for senior members of a Faculty/School.

6.11 Creating a Mailing List

Applicant shall send an Email to helpdesk@kafuco.ac.ke or ictsupport@kafuco.ac.ke with the following information:

i. Name of Applicant.
ii. Names of the subscribers
iii. Department.
iv. Contact Phone.
v. Name of List.
vi. Description of List.
vii. Name and Email Address of Moderator (if list will be moderated).

The mailing list will be created and the applicant notified either by Email or phone. This will normally be done within a day by the ICT Directorate.

ANNEX 7: WEBSITE GUIDELINES

The University College website(s) shall be maintained by the Webmaster and overseen by a Website Committee which shall meet regularly during the academic year. To ensure coherence across the website a protocol shall be established. The Registrar in charge of Administration shall be responsible for ensuring compliance with relevant legislation and with the University College's policies and standards regarding quality and presentation. This includes the accuracy of the content and ensuring that the site is kept up to date.

7.1 Website Governance

i. Website Manager (Webmaster): There shall be a Website Manager (Webmaster) who will provide quality assurance on the Content, Look and Feel of the University College Website ensuring that it is in tune with the University College’s mission, unique identity, core values and status.
ii. The Webmaster shall be responsible for setting policies governing the nature, content, format, maintenance, timeliness and ownership of information contained on the official pages of the website.
iii. Public Relations Office (PRO): The Public Relations Office (PRO) shall be responsible for maintaining the content of the Home and main web pages. Information to be put up on these main pages shall be routed through the PRO. The PRO shall then proof read and edit the content. It will have an officer designated as a Web Assistant. The Web Assistant shall be responsible for updating the website and responding to Emails.
iv. ICT Directorate: The ICT Directorate shall provide technical and advisory support services for the website. The ICT Directorate shall be responsible for maintaining the University College web server.

7.2 Website Structure and Content

The website shall be made up of the following web pages:

i. Main University College Web Pages: These shall comprise the University College Home Page and pages that provide:
   a) The profile of the University College, i.e., the governance structure, the courses and programmes of the Schools, Faculties, Institutes and Centres, as well as the administrative departments.
   b) Admission and registration processes and requirements.
   c) University College Policies and Regulations.
   d) News, events and announcements and any other relevant information
   e) Staff web portal
   f) Departmental Web Pages: These shall comprise the pages or website of the respective Schools, Faculties, Institutes and Centres of the University College. These pages shall provide details of the courses, programmes as well as academic staff. Personal web pages of Staff shall be set up under the Departmental websites.
   g) Student Web Portal: This shall be made up of pages that capture the life, programmes and activities of students.

h) Affiliates Websites: These are the websites of the affiliates of the University College that the University College may choose at its own discretion to have links.
i) Others Website: These are sites that the University College may have links to, for the purpose of collaboration.

7.3 Main University College Web Pages

i. The Public Relations Office shall be responsible for updating and maintaining the content of the main University College web pages.
ii. The content of the main University College web pages shall reside on the University College web server.

7.4 Departmental Web Pages

i. By default, where a Department does not have a website, a minimum number of web pages on the University College web server shall be allocated to publish information about the Department.
ii. The Public Relations Office in conjunction with the ICT Directorate shall create a standard set of pages for the Department. However, responsibility for maintaining information on the website shall rest with the Department's Administrative Assistant.
iii. Departments may choose to have a website of their own which may be hosted outside the University College web server. In this case a link will be established on the University College's website to the Department's site. Based on the policy provisions in this document, the Public Relations Office in consultation with the ICT Directorate shall approve of the establishment of links to departments that have established their own websites.
iv. The web pages of Department-owned websites shall comply with the policy provisions in this document. Websites that do not comply shall have their links removed. The decision shall be made by the Webmaster. This regulation applies to personal pages of Faculties.
v. The Public Relations Office shall ensure that information on all Departments, i.e., Schools, Faculties, Departments, Institutes or Centres is available on the website.

7.5 Student Web Portal

i. The student web portal shall be managed by the System Administrator
ii. The student web portal shall be hosted by the University College web server.
iii. For other student groups, the decision to link or host pages shall be at the discretion of the ICT directorate.

7.6 Websites of Affiliates and Others

i. Links to the websites of Institutions affiliated to the University College or otherwise shall be established at the discretion of the University College.

ii. The Public Relations Office shall conduct due diligence of the institution website using the provisions in this policy document and grant approval in consultation with the Webmaster.

7.7 Applications to link to University College Website

i. Outside institutions or organisations that wish to establish a link on their website to that of the University College shall apply to the Public Relations Office.
ii. The Public Relations Office shall conduct due diligence of the institution and their website using the provisions in this policy document and grant approval in consultation with the Webmaster.

7.8 General Guidelines for Web Pages

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

i. Content Management System: All web pages or websites shall have a Content Management System (CMS) which shall be used to update the information on the website.
ii. Identification: All web pages shall be identified by the University College logo or logotype.
iii. Contact Information: All web pages shall carry the Email address of the department or officer in charge for their upkeep. The Web Assistant/ Departmental Administrative Assistant shall check for Email and respond.
iv. Legal Compliance: All pages shall not violate the University College policy and statutes, copyright, libel, obscenity or other local or national laws.
v. Commercialisation: Web pages shall not be used for commercial purposes, sales or money-making ventures except those authorised by the University College administration.
vi. Accuracy and Currency: All pages shall be accurate, well-written, concise, and free of spelling and grammatical errors, and shall otherwise present the University College's mission and values in a positive light.
vii. Monitoring: All pages shall be regularly monitored by the Webmaster and Web Assistants to ascertain that material is current or appropriate. Outdated or inappropriate materials shall be removed within five working days when they are noticed.
viii. Enforcement of Website Policy:
    a) Any staff, student or individual that notices an error or considers content on the website to be inappropriate shall bring it to the attention of the Public Relations Office or Web Assistant in charge of the page.
    b) The Public Relations Office or Web Assistant shall take measures to address the concern and give a feedback to the complainant.
    c) The following shall govern the escalation procedures if the issue has far-reaching implications:
        i. Head/Secretary/Web Assistant of a department shall escalate to the Public Relations Office.
        ii. Public Relations Office escalates to Webmaster.
        iii. Webmaster escalates to the ICT Director.

iv. ICT Director escalates to ICT Advisory Committee.

d) Where an individual who reported a problem on the site is not satisfied, the complaint shall be escalated to the management board.

e) Any page on the University College site that violates the policy may be removed from the website immediately by the Web Assistant of the Department or Public Relations Office or the University College Webmaster.

ANNEX 8: ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES

These guidelines outline the acceptable use of University College Information Communication and Technology resources, which include, but are not limited to, equipment, software, networks, data, and stationary and mobile communication devices whether owned, leased, or otherwise provided by Kaimosi Friends University College. The guidelines aim at preserving access to information technology resources as a community effort which requires each member to act responsibly and guard against abuses. Therefore, both the community as a whole and each individual user have an obligation to abide by the standards established here for acceptable use.

8.1 User Responsibilities

i. Each user shall lawfully use only those information technology resources for which he or she has authorization. Violations include but are not limited to:
   a) using resources without specific authorization
   b) using another individual's electronic identity
   c) accessing files, data or processes without authorization

ii. Information Communication Technology resources must be used only for their intended purpose(s). Violations include but are not limited to:
   a) misusing software to hide personal identity, or to interfere with other systems or users
   b) misrepresenting a user’s identity in any electronic communication
   c) using electronic resources for deceiving, harassing or stalking other individuals
   d) sending threats, “hoax” messages, chain letters, or phishing
   e) intercepting, monitoring, or retrieving without authorization any network communication
   f) using University College computing or network resources for advertising or other commercial purposes
   g) circumventing or attempting to circumvent security mechanisms
   h) using privileged access to University College systems and resources for other than official duties directly related to job roles and responsibilities
   i) making University College systems and resources available to those not affiliated with the University College
   j) using former system and access privileges after association with the University College has ended

iii. The access to and integrity of information communication technology resources must be protected. Violations include but are not limited to:
   a) creating or propagating computer viruses, worms, Trojan Horses, or any other malicious code
   b) preventing others from accessing an authorized service
   c) developing or using programs that may cause problems or disrupt services for other users
   d) degrading or attempting to degrade performance or deny service
   e) corrupting or misusing information
   f) altering or destroying information without authorization

iv. Applicable state laws and University College policies must be followed. Violations include but are not limited to:
  a) failure to respect the copyrights and intellectual property rights of others
  b) making more copies of licensed software than the license allows
  c) downloading, using or distributing illegally obtained media (e.g., software, music, movies)
  d) uploading, downloading, distributing or possessing child pornography
  e) accessing, storing or transmitting information classified as Restricted data (e.g., social security numbers, patient health information, driver's license numbers, credit card numbers) without a valid business or academic reason or transmitting such information without using appropriate security protocols (e.g., encryption).
  f) Using third party email services (e.g. Hotmail, Yahoo) or non-encrypted email services to transmit University College information classified as Restricted.
  g) Forwarding or auto-forwarding restricted information to a non-KAFUCO email service.
  h) Distributing information classified as restricted, unless acting as an authoritative University College source and an authorized University College distributor of that information and the recipient is authorized to receive that information.
  i) Using media tools (e.g., Facebook, YouTube,) to communicate or store University College information classified as restricted.
  j) Using third party cloud storage or data sharing tools (e.g. iCloud, Carbonite, Dropbox) to store University College information classified as restricted.

v. Users must respect the privacy and personal rights of others. Violations include but are not limited to:
  a) accessing, attempting to access, or copying someone else's electronic mail, data, programs, or other files without authorization.
  b) divulging sensitive personal data to which users have access concerning faculty, staff, or students without a valid business or academic reason.

8.2 Privacy

The University College recognizes that all members of the University College Community have an expectation of privacy for information in which they have a substantial personal interest. However, this expectation is limited by the University College's needs to obey applicable laws, protect the integrity of its resources, and protect the rights of all users and the property and operations of the University College. The University College reserves the right to examine material stored on or transmitted through its information communication technology facilities if there is reason to believe that the standards for acceptable use are being violated, or if there is reason to believe that the law or University College policy are being violated, or if required to carry on its necessary operations.

Reasonable efforts will be made to notify the user of the need for access to information in which he or she has a substantial personal interest stored on or transmitted through the University College's information communication technology resources unless prohibited by law, inconsistent with University College policy, or inconsistent with the University College carrying out its normal operations.

8.3 Exemptions

These exemptions shall apply under special circumstances where investigations are proposed to be undertaken further user support may be sought from the relevant authority. Where there is no explicit waiver as provided above, inappropriate use of Kaimosi Friends University College ICT resources will lead to disciplinary action and legal proceedings being taken against the user.

ANNEX 9: BUSINESS CONTINUITY MANAGEMENT

The purpose of these policy guidelines is to ensure server and data continuity and to support the retrieval and restoration of archived information in the event of a disaster, equipment failure, and/or accidental loss of files. The University College at a minimum will:

a) establish plans and processes to assess the risk and impact of the loss of Information and ICT Assets on University business in the event of a disaster or security failure and develop methods for reducing known risks to University Information and ICT Assets
b) ensure business continuity Information and ICT Asset disaster recovery plans are maintained and tested to ensure Systems and Information are available and consistent with agency business and service level requirements.

The ICT Director is responsible for providing policy-based, system level, network-based backups of server systems.

9.1 System Backup Profiles

The ICT Directorate shall maintain the following type of backup profiles:

9.2 Standard Backup

The standard backup is provided for most centralized University College computer systems. The backup could be full, differential or incremental. The frequency of backup could be daily, weekly or monthly and is dependent upon the application. The retention of these backups could vary from 1 week up to 2 months. For some applications, backup is performed on a day and time agreed upon by the ICT Directorate and application owner.

9.3 Critical System Backup

Certain enterprise-wide systems are deemed critical to University College operations and dictate longer retention periods from 6 months up to 1 year. The type, frequency and retention period is different for different applications. Prior to a major upgrade of a production system, database, or application, a full system backup is performed and retained for 6 months.

9.4 Special Request Backup

Some departments or applications may require an exception to the standard backup retention periods mentioned above. Exceptions are permitted, but must be fully documented.

9.5 Storage Locations and Retention

Unless a system supporting an application or business function requires a custom retention period, the ICT Directorate will maintain full and incremental backups.

Backup tapes for the current weekly backup period will be stored within the DICT for purposes of current backups and restores.
Tapes representing backups from the former weekly backup period will be stored within a secured, fireproof place until such time as the backup images stored on these tapes expire and the tapes are re-used or destroyed.

After a successful backup, it will be stored in a secure, off-site media vaulting location for an appropriate period for disaster recovery purposes. This will ensure that no more than one week of information would be lost in the event of a disaster in which campus systems and backup images are destroyed. After the period of six months has elapsed, the tapes may 'optionally' be returned to ICT Directorate and re-used or destroyed.

9.6 Backup Verification

On a periodic basis, logged information generated from each backup job will be reviewed for the following purposes:

a) to check for and correct errors
b) to monitor duration of the backup job
c) to optimize backup performance where possible

The ICT Directorate will identify problems and take corrective actions to reduce any risks associated with failed backups. Test restores from backup tapes for each system will be performed. Problems will be identified and corrected. This will work to ensure that both the tapes and the backup procedures work properly

DICT will maintain records demonstrating the review of logs and test restores so as to demonstrate compliance with this policy for auditing purposes.

9.7 Media Management

Media will be clearly labelled and logs will be maintained identifying the location and content of backup media. Backup images on assigned media will be tracked throughout the retention period defined for each image. When all images on the backup media have expired, the media will be re-incorporated amongst unassigned (available) media until reused. Periodically and according to the recommended lifetime defined for the backup media utilized, ICT Directorate will retire & dispose of media so as to avoid media failures.

9.8 Storage, Access and Security

All backup media must be stored in a secure area that is accessible only to designated University College staff or employees of the contracted secure off-site media vaulting vendor used by ICT Directorate. Backup media will be stored in a physically secured, fireproof place when not in use. During transport or changes of media, media will not be left unattended.

9.9 Retirement and Disposal of Media

Prior to retirement and disposal, DICT will ensure the following:

a) the media no longer contains active backup images or that any active backup images have been copied to other media

b) the media's current or former contents cannot be read or recovered by an unauthorized party.
c) with all backup media, CICT will ensure the physical destruction of the media prior to disposal.

9.10 Disaster Recovery Considerations

As soon as is practical and safe post-disaster, ICT Directorate will:

a) Restore existing systems to working order or obtain comparable systems in support of defined business processes and application software.
b) Restore the backup system according to documented configuration so as to restore server systems.
c) Obtain all necessary backup media to restore server computing systems
d) Restore server computing systems according to the priority of systems and processes as outlined for restoration and recovery in the Disaster Recovery Plan

9.11 Documentation

Essential documentation shall be maintained for orderly and efficient data backup and restoration. The person-in-charge of data backup should fully document the following items for each generated data backup:

S/No.	Action Item	Action
	Date of data backup	
	Type of data backup (incremental, differential, full)	
	Number of generations	
	Responsibility for data backup	
	Extent of data backup (files/directories)	
	Data media on which the operational data are	
	Data media on which the backup data are stored	
	Data backup hardware and software (with version) number	
	Storage location of backup copies	

ANNEX 10: SOCIAL MEDIA GUIDELINES

Social media encompasses a wide, and constantly changing, variety of electronic communications tools and sites which facilitate digital creation and interaction. This policy guideline is designed to provide University College members and employees with guidance in using social media to communicate professionally.

Social media accounts set up in the name of the University College, or attributable to the University College, can provide a fast route for feedback, comments and ideas. As such, this facility provides a valuable forum for discussion. Unfortunately, it is open to abuse and can in extreme cases lead to reputational damage to the Institution or individual defamation of character and subsequent legal action. With this in mind, all University College related social media accounts (Facebook, twitter etc.) should have a key administrator who takes responsibility for the account and who is responsible for granting write (administrator) access to the account.

The University College Webmaster is to be the key administrator on all such University College accounts and should hold account details and any necessary passwords. As a rule, there is a need to be careful over copyright, trademarks, data protection and the use of logos. In addition, in the interests of security, users should avoid revealing personal information where possible, avoid any dialogue with journalists and avoid unsubstantiated claims.

10.1 Application of the Policy

If members and staff are creating or contributing to blogs, microblogs, wikis, social networks, or commenting on a post on a site, or if they are using any other kind of social media to communicate and they are identifiable as a University College member or employee then this policy will be applicable. The way in which social media sites are facilitated makes it even more difficult to differentiate between use in professional and personal capacities than say the telephone or the Internet. It is important to note that this policy applies even to personal use of social media where a member or an employee is identifiable as an employee of the University College.
In particular, staff or members who:

1. Actively manage and maintain a social media presence on behalf of one of the University College departments, activities or a affiliated projects;
2. Contribute comments, reviews and content to social media sites, forums, networks including those for personal use. Examples include:
    a. Maintaining a profile page on one of the social networking sites (such as LinkedIn or Facebook) where the individual is identified as a member or employee of the College or an affiliated project;
    b. Displaying an @kafuco.ac.ke e-mail address or listing University College or an affiliated projects as the individuals place of work;
    c. Joining a University College network on a social media site;
    d. Actively running a personal blog that covers aspects of the individual’s professional work.

e. Communicate University College's participation in any forms of social media, such as when speaking at a conference, giving a presentation, running a training course, taking part in case studies etc.

10.2 Social Media Terms and Conditions

Each social media site will have its own terms and conditions for use and it is the responsibility of each individual using the site to follow those terms of use. For example, Facebook does not permit multiple personal accounts.

10.3 Confidential or Reserved Information

Care should be taken to avoid revealing information on College or personal sites or tools that might compromise the University College in any way. Individuals should not post:

i. Personal or commercially sensitive information;
ii. Product or service developments;
iii. Business strategy;
iv. Current legal proceedings;
v. Offensive, pornographic or indecent content;
vi. Images of anyone under the age of 18 without the express parental consent;
vii. Anything that may bring the University College into disrepute.

10.4 Posting content for University College

When publishing content, posts or updates to the University College social media sites, it is helpful to remember the reasons for doing so. When using University College social media sites, the aims should be to:

a. Promote the Colleges activities;
b. Reach a wider, more diverse audience than the website alone;
c. Educate, inform and entertain;
d. Endorse the teaching and research of University Fellows and academic staff;
e. Promote debate with a view to finding solutions
f. Consider alternative viewpoints;
g. Promote activities events.

ANNEX 11: ICT ACQUISITION GUIDELINES

The following guidelines are provided for the acquisition of IT hardware, software and networking products and services. When in doubt, user Departments shall consult the ICT Directorate for clarification or advice. The ICT Directorate shall use standards and specifications for computer equipment and software as provided by the Communication Authority of Kenya (CAK):

i. **Warranty**: A minimum of one (1) year warranty shall be specified for all technology acquisitions.
ii. **Laptop and Desktop Computers:** Computers purchased shall have sufficient capacity to run applications at satisfactory response time for at least the next 5 years.
iii. **Proven Technology:** Only proven hardware and software with available and very well established support shall be acquired. Preference shall be on proven technology, not leading edge.
iv. **Industry Standards Based:** Technologies that conform to international industry standards shall be adopted. This will apply to hardware, networks, operating systems, databases and portable software. Proprietary technology and tools shall be avoided where industry standard systems exist.
v. **Compatibility:** New technology components shall be compatible with one another and with the existing ICT systems.
vi. **Upgradeability and Scalability:** Technology components acquired shall be upgradeable or scalable.
vii. **Security:** The Technology component or system shall have industry standard security built in.

11.1 Purchase of computers and related equipment

The ICT Directorate shall recommend the specifications for servers, workstations, PCs and related equipment purchased by the University College's Procurement Office in accordance with the Public Procurement and Assets Disposal Act, 2015 and the Public Procurement and Disposal Regulations, 2015 and ICT standards as published by ICT Authority from time to time.

11.2 Purchase or Lease

It is the policy of the University College to purchase rather than lease computers or lease high-end servers. However, on a need basis, especially for short term use, a lease arrangement can be agreed on with the approval of the Principal.

Laptops and notebooks purchase is limited and staff members are encouraged to buy their own laptops. Staff will get support to buy their own laptops on a check-off basis, under a scheme to be initiated by the University College administration with the approval of Council.

The University College will participate in projects sponsored by the private or public sector to enhance student access to laptops and PCs. The terms and conditions for participating in such projects will be vetted by the ICT Advisory Committee on behalf of the University College.

11.3 Equipment Donations

Donations of computers and other ICT equipment made to the University College shall be guided by the Corporate Social Responsibility guidelines. They will be accepted if the equipment meets the immediate needs of the University College. The ICT Directorate will verify the specifications of the donated equipment, in consultation with the department or unit where the equipment will be deployed. The University College shall reserve the right to accept or reject equipment donation.

11.4 Educational Discounts

The University College will actively solicit educational discounts from manufacturers of branded hardware and or software. Such discounts will be negotiated a priori with such manufacturers or software houses as part of their documented corporate policy. The University College will pay careful attention to the Terms and Conditions associated with such discounts.

11.5 Service Contract

i. User Departments are advised to consult the ICT Directorate and the Legal Office before any contract with any ICT service provider is consummated.
ii. The ICT Directorate shall publish Contract Templates that may be adopted for ICT service contracts.

ANNEX 12: IT PROJECT MANAGEMENT GUIDELINES

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

12.1 Project Implementation Team

i. All IT Projects shall have a properly constituted Project Implementation Team (PIT).

ii. For a University College-wide project, the PIT shall be constituted by the Principal

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

iv. The PIT shall comprise:
   - a) Project Sponsor – The Principal, Dean, or Head where applicable.
   - b) Project Manager – Preferably shall be appointed from the faculty or department that is the direct beneficiary of the project.
   - c) Project Team – Depending on the nature and scope of the project, the team shall be cross-functional (i.e., a mix of Faculty, ICT Directorate, etc.)

v. The following shall form the phases of the project:

   I. Project Initiation
   - a) Project justification and approval process resulting in an approved budget.
   - b) There shall be a Project Definition Document that defines at least the goals, objectives, resources to be used, deliverables and time frame of the project.
   - c) Identification and selection of Project Team members.
   - d) Definition of roles and responsibilities.

   II. Project Planning
   - a) Preparation of detailed plans for managing the project.
   - b) The planning phase shall be used to define the project infrastructure – project filing and documentations and the various procedures for managing the issues, quality, risks, reporting and communications.

   III. Project Execution
   - a) Monitoring and controlling the project plan.
   - b) Issuing status reports.

   IV. Project Closure

   Formally handing over deliverables and issuing Project Completion Report.

ANNEX 13: ICT INFRASTRUCTURE AND SYSTEMS CHANGE MANAGEMENT GUIDELINES

The purpose of these policy guidelines is to establish management direction and high-level objectives for ICT change management. This policy will ensure the implementation of change management strategies to mitigate associated risks such as:

a) Information being corrupted or destroyed
b) Computer performance being disrupted or degraded
c) Productivity losses being incurred
d) Exposure to reputational risk

The change management process shall be formally defined and documented, to control changes to all critical information resources (such as hardware, software, system documentation and operating procedures). This process shall include management responsibilities and procedures. Wherever practical, operational and application change management procedures should be integrated.
At a minimum the change management process shall include the following phases:

i. Logged Change Requests
ii. Identification,
iii. Prioritisation and initiation of change
iv. Proper authorisation of change
v. Requirements analysis
vi. Interdependency and compliance analysis
vii. Impact Assessment
viii. Change approach
ix. Change testing
x. User acceptance testing and approval
xi. Implementation and release planning
xii. Documentation
xiii. Change monitoring
xiv. Defined responsibilities and authorities of all users and ICT personnel
xv. Emergency change classification parameters

13.1 Documented Change

a) All change requests shall be logged whether approved or rejected on a standardised and central system. The approval of all change requests and the results thereof shall be documented.
b) The ICT Division shall maintain a documented audit trail, containing relevant information at all times. This should include change request documentation, change authorisation and the outcome of the change. No single person should be able to effect changes to production information systems without the approval of other authorised personnel.

13.2 Risk Management

a) A risk assessment shall be performed for all changes and depending on the outcome, and impact assessment should be performed.
b) The impact assessment shall include the potential effect on other information resources and potential cost implications. The impact assessment should, where applicable consider compliance with legislative requirements and standards.

13.3 Change Classification

All change requests shall be prioritised in terms of benefits, urgency, effort required and potential impact on operations.

13.4Testing

Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimise the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made.

13.5 Changes Affecting Service Level Agreements

The impact of change on existing Service Level Agreements (SLA) shall be considered. Where applicable, changes to the SLA shall be controlled through a formal change process which includes contractual amendments.

13.6 Version Control

Any software change or update shall be controlled with version control. Older versions shall be archived

13.7 Approval

All changes shall be approved prior to implementation. Approval of changes shall be based on formal acceptance criteria i.e. the change request was done by an authorised user, the impact assessment was performed and proposed changes were tested.

13.8 Communicating Changes

All users, significantly affected by a change, shall be notified of the change. The user representative shall sign-off on the change request form. Users shall be required to make submissions and comment prior to the acceptance of the change.

13.9 Implementation

Implementation will only be undertaken after appropriate testing and approval by Change Management Committee. All major changes shall be treated as new system implementation and shall be established as a project. Major changes will be classified according to effort required to develop and implement said changes.

13.10 Fall Back

Procedures for aborting and recovering from unsuccessful changes shall be documented. Should the outcome of a change be different to the expected result (as identified in the testing of the change), procedures and responsibilities shall be noted for the recovery and continuity of the affected areas. Fall back procedures shall be in place to ensure systems can revert back to what they were prior to implementation of changes.

13.11Documentation

Information resources documentation shall be updated on the completion of each change and old documentation shall be archived or disposed of as per the documentation and data retention policies. Information resources documentation is used for reference purposes in various scenarios i.e. further development of existing information resources as well as ensuring adequate knowledge transfer in the event of the original developer or development house being unavailable. It is therefore imperative that information resources documentation is complete, accurate and kept up to date with the latest changes. Policies and procedures, affected by software changes, shall be updated on completion of each change.

13.12 Disaster Recovery Plan (DRP)

The Disaster Recovery Plan shall be updated with relevant changes, managed through the change control process. The Disaster Recovery Plan and continuity plans rely on the completeness, accuracy and availability of DRP documentation. DRP documentation is the road map used for minimal disruption in business continuity.

14.13 Emergency Changes

Specific procedures to ensure the proper control, authorisation, and documentation of emergency changes shall be in place. Specific parameters will be defined as a standard for classifying changes as Emergency changes.

13.14 Change Monitoring

All changes shall be monitored once they have been rolled-out to the production environment. Deviations from design specifications and test results will be documented and escalated to the solution owner for ratification.

13.15 Roles and Responsibilities

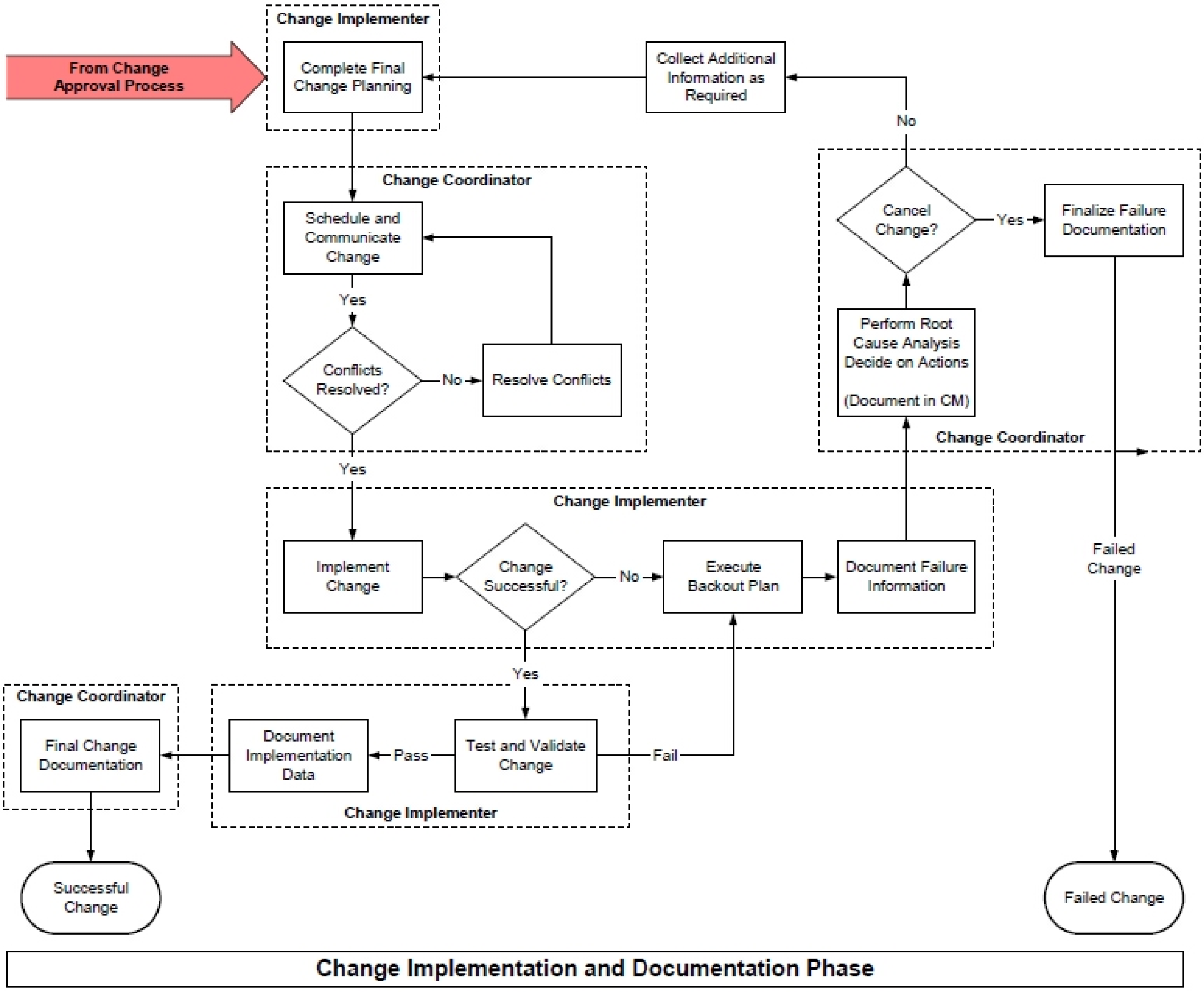
13.15.1 Change Management Committee

Ensure that the necessary information security controls are implemented and complied with as per this policy

13.15.1 ICT Director

a) Approve and authorize change management procedures
b) Ensure that all users are aware of the applicable policies, standards, procedures and guidelines for change management
c) Ensure that policy, standards and procedural changes are communicated to applicable users and management
d) Evaluate change request and potential risks and introduce counter measures to address these risks
e) Facilitate and coordinate the necessary change management procedures within the Municipality
f) Report and evaluate changes to change management policies and standards
g) Coordinate the implementation of new or additional security controls for change management
h) Review the effectiveness of change management strategy and implement remedial controls where deficits are identified
i) Coordinate awareness strategies and rollouts to effectively communicate change management mitigation solutions
j) Establish and revise the information security strategy, policy and standards for change management
k) Evaluate incidents and potential risks to the Municipality and facilitate the necessary counter measures to change management initiatives and evaluate such policies and standards
l) Coordinate the overall communication and awareness strategy for change management
m) Coordinate the implementation of new or additional security controls for change management.

13.16 Change Management Work Flow


From Change Approval Process
Change Implementer
Complete Final Change Planning
Collect Additional Information as Required
No
Change Coordinator
Schedule and Communicate Change
Yes
Conflicts Resolved?
No
Resolve Conflicts
Yes
Cancel Change?
Yes
Finalize Failure Documentation
Perform Root Cause Analysis Decide on Actions (Document in CM)
Change Coordinator
Change Implementer
Implement Change
Change Successful?
No
Execute Backout Plan
Document Failure Information
Failed Change
Yes
Change Coordinator
Final Change Documentation
Document Implementation Data
Pass
Test and Validate Change
Fail
Change Implementer
Successful Change
Failed Change
Change Implementation and Documentation Phase

ANNEX 14: END USER SKILLS DEVELOPMENT GUIDELINES

End-user skills development includes all efforts to enforce awareness, general knowledge and general and specific computer skills related to the use of information technology. Within this context the end-user is defined as each person who uses ICT services or the information they produce to support his/her “normal” learning, teaching, research, administrative, secretarial, or managerial tasks.

In order to facilitate the implementation of the different ICT services and systems, considerable knowledge and skills must be developed among all levels of potential users. This will enable them to use ICT services and systems effectively and independently, and also to be aware of the shared responsibilities. In line with the implementation of the different ICT services and systems, considerable knowledge and skills will have to be developed among the end-users so that they are able to:

a) Use ICT services and systems effectively and as independently as possible.
b) Contribute to the specification, design and implementation of ICT applications.
c) Be aware of the shared responsibilities for equipment, software and data, and enforce an atmosphere of collective responsibility and system ownership.
d) Manage and control complex project oriented processes, like implementing University College-wide infrastructure or information systems.
e) Establish and sustain effective, efficient application and data management and systems maintenance.

The University College will require that all students, academic staff, administrative and support staff are trained on a continuing basis to equip them with the requisite skills to exploit the functional potential of ICT. It is expected that as a minimum standard, all staff and students will be able to use standard application packages (word processors, spreadsheets and databases), e-mail and the Internet.

The University College shall provide for the development and implementation of a consistent set of training programs with different levels for different categories of (potential) ICT users: Students, teaching and research staff, clerical and secretarial staff, and general management staff.

Additionally, the University College shall create organizational (trainer capacity, training management) and technical (practice lab and computer based training tools, self-paced training mode) conditions assuring continuous in-house ICT training capabilities in the long-term.

Training shall be provided to cover, as far as possible, all skill levels. While it is not intended to turn all users into experts, it is held that the training plan supports all users at all levels. It would be inadequate to only support the least advantaged group, as that would have the undesirable effect of creating a great mass of ‘average’ users with no experts. The need for experts is never diminished.

The short- and medium-term goals shall be aimed at creating, as rapidly as possible, a sizeable proportion of staff who are familiar with, and able to effectively use the ICT infrastructure in their daily work. At the end of the first phase of the training, the University College expects that:

a) All students and staff at all levels are able to use standard application packages (word processors, spread sheets, data bases) as well as email and the Internet.
b) Routine administrative tasks like calling like calling meetings and distribution of minutes and other documents are handle via email
c) Students and staff interact more using online message boards, email, and online discussion fora. The traditional modes of interaction (notice boards, circulars) should be replaced for most activities.

14.1 Administration of Training

a) 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
b) The number of staff to be trained shall be as targeted in the Strategic Plan for the University College. The University College shall make the necessary arrangements to facilitate trainees drawn from such Departments.
c) The University College shall provide necessary resources to facilitate the training.
d) The ICT Directorate shall develop topics for all training including development or sourcing of training material. These shall include but are not limited to:-
    i. Where possible provide training materials on-line via the University College website or intranet.
    ii. Where possible conduct on-line assessment tests and examinations via the University College intranet.

14.2 Training Resources

In order for the above to have a good chance of being effective, the University College needs well-equipped training facilities. At the moment there are a number of computer labs scattered around the University College that could be used for the training. One fully equipped training center will be set up at the University College, to be used as needed for training purposes.

The training centre, to be owned by the Directorate of ICT, shall include state-of-the-art equipment and software. The University College will provide space for the training center.

To better support learning, online applications for user support will also be developed. These will include moderated online discussion fora where users can ask questions, share ideas and solutions and basically keep in touch; online manuals and Frequently Asked Questions (FAQ) lists. This approach will enhance information sharing as well as increasing user familiarity with using online resources.

ANNEX 15: DATA AND INFORMATION GUIDELINES

i. The University College shall endeavour to protect the confidentiality of information and material furnished by the user and shall instruct all computing personnel to protect the confidentiality of such information and material, but the University College shall be under no liability in the event of any improper disclosure.
ii. Recording or processing information which infringes any patent or breaches any copyright shall be avoided. Individual persons, not the University College, shall be held responsible for any patent or copyright breaches.
iii. All information acquired or created by user while carrying out the University College's business, except that which is specifically exempted as private or personal, is a general University College resource. However, each User Department shall have individual ownership of its own data resource.
iv. Single Source Principle: Data shall be captured at source to avoid data re-input error and duplication.
v. Data Accuracy: Each user shall be responsible for the accuracy of the data that they enter into the system and they shall own it.
vi. Users accept the following specific responsibilities:
    a) Security
        i. To safeguard their data, personal information and confidential data.
        ii. To take full advantage of file security mechanisms built into the computing systems.
        iii. To follow the security policies and procedures established to control access to and use of data.
    b) Confidentiality
        i. To respect the privacy of other users; for example, not to intentionally seek or access information on, obtain copies of, or modify data belonging to other users.
        ii. Not to divulge sensitive personal data concerning staff or users to which they have access without explicit authorisation to do so.
        iii. Not to access information and data without proper authority, nor make unauthorised modifications to the contents of any computer system, including deleting or changing data.
        iv. Not to disclose or use computerised personal data for any purpose which contravenes national or international legislation.

Individuals who violate any of these directives stated above are subject to discipline up to and including termination from employment, in accordance with employment contract, professional discipline or criminal prosecution in accordance with the laws of the country. At the discretion of the Principal, the University College may terminate an employee or student for the first, substantiated breach of its confidentiality and security policy if warranted by the seriousness of that breach. Any employee or student who believes that another staff member, student or employee has breached the confidentiality or integrity of one's information or the University College's information or data shall immediately report that breach to the appropriate authority. The Chief Security Officer shall instruct to be conducted a thorough and confidential investigation of the allegation and recommend corrective action to the Principal.

The Chief Security Officer shall inform the complainant of the results of the investigation and any corrective action taken. The University College shall not retaliate against or permit reprisals against any staff or student who reports a suspected violation of its policies protecting the confidentiality and integrity of personnel or University College's information and data.

vii. Data Backups Strategy

a) A backup strategy and procedures shall be established to allow computer systems to recover from effects, which impair availability of and access to system functions and data. The chosen backup strategy shall aim to restore services within a specified acceptable period of downtime, driven by KAFUCO business objective, economic and justifiable recovery environment.
b) In order to ensure prompt and easy recovery from data loss/corruption it is necessary to keep reliable backups of all documents and data.
c) Both on-site and off-site backups need to be kept.
d) Regularly test the backup media to ensure that the media can be read and can be relied upon for emergency use when necessary.
e) All data backup tapes/CDs/disks shall be stored in a secure location (eg, fireproof safe) and this environment shall be conducive to storage of magnetic media. Documents will be archived on a monthly basis.

ANNEX 16: ICT GOVERNANCE AND SERVICE MANAGEMENT

16.1 Responsibilities

ICT services in the University College shall be managed by the:-

i. ICT Directorate.
ii. ICT Advisory Committee.
iii. ICT Help Desk.

16.1.1 ICT Directorate

The ICT Directorate is mandated to provide leadership in the development, management and use of ICT in the University College as follows:-

i. Development and implementation of ICT Policies, Strategies and Standards.
ii. Support of the University College's ICT Infrastructure. This covers the management and day-to-day operation of the:
   a) Network Operation Centre.
   b) University College's backbone network that interconnects the Local Area Networks (LANs).
   c) Telephone system.
   d) University College Website
iii. The setup, administration, troubleshooting and problem resolution of personal computers, printers, servers, networks and communications systems.

16.1.2 Head of the ICT Directorate

The ICT Directorate will be headed by the Director ICT who will be answerable to the University College Deputy Principal (Administration, Finance, Planning and Development) and the Principal, or as provided in the University College Statutes.

16.2 ICT Advisory Committee

University College Management shall appoint members of the ICT Advisory Committee. The functions of the ICT Advisory Committee shall be to:-

a) Offer advice on the formulation of policies and guidelines for the running of the ICT Directorate.
b) Oversee the administration of the ICT Directorate.
c) Make recommendations to the Management Board on the use of ICT facilities in the University College.
d) Offer advice on the development of ICT infrastructure and acquisition of computers and ICT equipment.

16.3 ICT Help Desk

The ICT Help Desk shall be created by the ICT Directorate and shall be the basis for managing problems and changes. Help Desk procedures shall be established for receiving user problems and requests, trouble ticketing and tracking, as well as problem resolution and escalation.

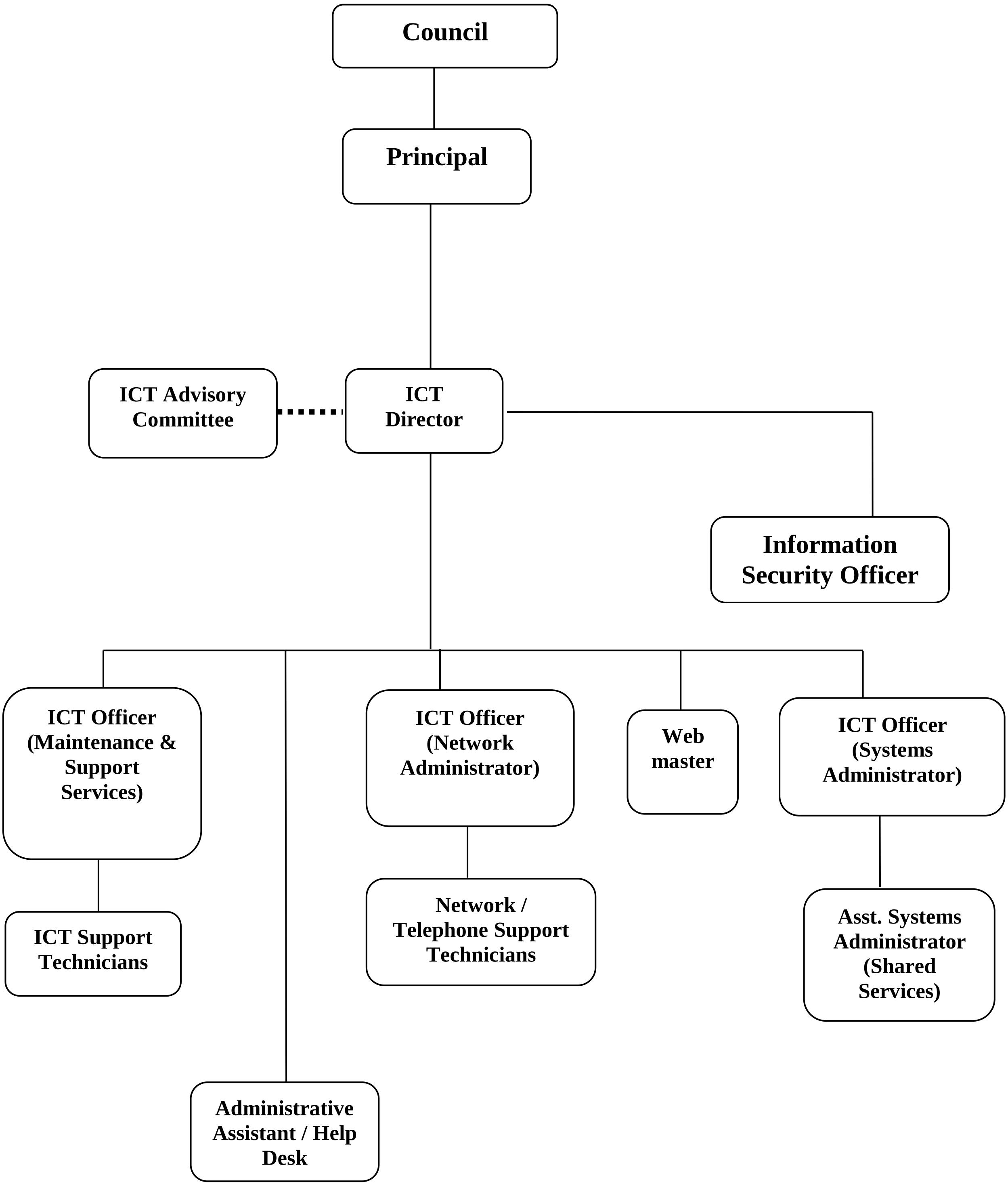
16.3.1 Objective

The objective of the ICT Help Desk shall be to provide customer-oriented ICT services to the KAFUCO user community by receiving problem calls, requests and enquiries, and arranging to have them resolved or addressed by the appropriate ICT personnel.

16.3.2 Service Availability

The Help Desk service shall be available during working hours. The Help Desk can be reached either through the University College hotline numbers or Email: helpdesk@kafuco.ac.ke or ictsupport@kafuco.ac.ke.

ANNEX 17: ICT DIRECTORATE ORGANOGRAM


Council
Principal
ICT Advisory Committee
ICT Director
Information Security Officer
ICT Officer (Maintenance & Support Services)
ICT Officer (Network Administrator)
Web master
ICT Officer (Systems Administrator)
ICT Support Technicians
Network / Telephone Support Technicians
Asst. Systems Administrator (Shared Services)
Administrative Assistant / Help Desk

ANNEX 18: COMPLIANCE AGREEMENT FORM

I, …. ……………………………………………………………..………………….
(PRINT FULL FIRST, MIDDLE & SURNAME – BLOCK LETTERS and in INK)

(a) acknowledge that I have read and understood the *KAFUCO ICT Policy*
(b) agree to abide by the requirements for access and use of these resources
(c) acknowledge that the ICT Department may authorise access to user logs in the event that there is a perceived threat to the:

- System security
- Privacy of staff
- Privacy of others
- Legal liability of the Kaimosi Friends University College

This signed acceptance is valid for the period of employment with KAFUCO or until a revised statement is deemed to be necessary as determined by the Kaimosi Friends University College Management

Signature:…………………………………………………………………

Date: …………………………………………………………………….

Department:…………………………………………………………….

Designation:…………………………………………………………….

PF No:…………………………………………………………………….

Note: Use of the full name is important. It must match personnel records of Human Resources Department. Do not use abbreviated or unless it is your formal name.

Please send this form to the ICT Director or email to ictd@kafuco.ac.ke

ANNEX 19: REFERENCES

The following policy documents variously informed the process of drafting the KAFUCO ICT Policy:

1. KAFUCO Statutes
2. KAFUCO Strategic Plan (2013-2018)
3. National Information and Communication Technology ICT Policy 2006
4. Jomo Kenyatta University of Agriculture and Technology ICT Policy
5. Makerere University ICT policy and master plan
6. Maseno University ICT Policy
7. University of Mines and Technology, Tarkwa ICT Policy
8. Jaramogi Oginga Odinga University of Science and Technology ICT Policy
9. Kibabii University College Draft ICT policy
10. University of Sydney policy on use of ICT resources
11. Bradford University ICT Strategy
12. University of Greenwich Rules and Regulations for Use of ICT
13. University of Nairobi ICT Policy