



KMTC is ISO 9001:2015 Certified

Kenya Medical Training College



INFORMATION & COMMUNICATION TECHNOLOGY
POLICY

MAY 2019

TABLE OF CONTENTS

PREFACE	i
FOREWORD	ii
DEFINITION OF TERMS	iii
ABBREVIATIONS	iv
1.0 INTRODUCTION	1
1.1 Preamble	1
1.2 Statement of Purpose	1
1.3 Objectives	1
1.4 Scope	2
1.5 Enforcement	2
2.0 PASSWORD	3
2.1 Introduction	3
2.2 Scope	3
2.3 Application	3
2.4 Purpose	3
2.5 Policy Statements	3
2.6 Guidelines	3
2.7 Enforcement	4
3.0 MALWARE	4
3.1 Introduction	4
3.2 Purpose	4
3.3 Scope	4
3.4 Application	4
3.5 Policy Statement	5
3.6 Guidelines	5
3.7 Enforcement	5

4.0 PHYSICAL SECURITY	5
4.1 Introduction.....	5
4.2 Scope.....	5
4.3 Application.....	6
4.4 Purpose	6
4.5 Policy Statement.....	6
4.6 Guidelines.....	6
4.7 Enforcement.....	7
5.0 LOGICAL SECURITY	7
5.1 Introduction.....	7
5.2 Scope.....	7
5.3 Application.....	7
5.4 Purpose	7
5.5 Policy statement.....	8
5.6 Guidelines.....	8
5.7 Enforcement.....	9
6.0 BACK-UP OF DATA AND INFORMATION	9
6.1 Introduction	9
6.2 Purpose	9
6.3 Scope	9
6.4 Application	9
6.5 Policy Statement.....	9
6.6 Guidelines.....	9
6.7 Enforcement	10
7.0 EMAIL	10
7.1 Introduction.....	10

7.2 Scope.....	10
7.3 Application.....	10
7.4 Purpose	10
7.5 Policy Statement.....	11
7.6 Guidelines for Acceptable E-mail use	11
7.7 Enforcement.....	11
8.0 INTERNET	11
8.1 Introduction.....	11
8.2 Purpose	11
8.3 Scope.....	12
8.4 Application	12
8.5 Policy Statement.....	12
8.6 Guidelines	12
8.7 Compliance	13
9.0 SOFTWARE ACQUISITION, DEPLOYMENT AND USE	13
9.1 Introduction.....	13
9.2 Purpose	13
9.3 Scope.....	13
9.4 Application	13
9.5 Policy Statement.....	13
9.6 Guidelines	13
9.7 Enforcement	14
10.0 MAINTENANCE AND SUPPORT.....	15
10.1 Introduction	15
10.2 Purpose.....	15

10.3 Scope	15
10.4 Application	15
10.5 Policy Statement	15
10.6 Guidelines	15
10.7 Enforcement	16
11.0 NETWORK DEVELOPMENT, DEPLOYMENT AND USE.....	16
11.1 Introduction	16
11.2 Purpose.....	16
11.3 Scope	16
11.4 Application	17
11. 5 Policy Statements.....	17
11.6 Guidelines	17
11.7 Enforcement	17
12.0 ICT TRAINING	17
12.1Introduction.....	17
12.2 Purpose	17
12.3 Scope	18
12.4 Application	18
12.5Guidelines.....	18
13.0 ICT GOVERNANCE	18
13.1 Introduction	18
13.2 Purpose	18
13.3 Scope	18
13.4 Application	18
13.5 Guidelines	18
13.6 Compliance	19

14.0 ACQUISITION, USE & DISPOSAL OF ICT EQUIPMENT	19
14.1 Introduction	19
14.2 Purpose	19
14.3 Scope	19
14.4 Application	19
14.5 Policy Statement	19
14.6 Guidelines	19
14.7 Enforcement	20
15.0 WEBSITE	20
15.1 Introduction	20
15.2 Purpose	20
15.3 Scope	20
15.4 Application	20
15.5 Policy Statement	20
15.6 Guidelines	20
16.0 COMPUTER LABORATORY USE AND SECURITY	21
16.1 Introduction	21
16.2 Scope	21
16.3 Purpose	21
16.4 Application	21
16.5 Policy Statement	21
16.6 Guidelines	21
16.7 Enforcement	21
17.0 DISASTER RECOVERY	22
17.1 Introduction	22
17.2 Scope	22

17.3 Purpose	22
17.4 Application	22
17.5 Policy Statement	22
17.6 Guidelines	22
17.7 Enforcement	23
18.0 SOCIAL MEDIA	23
18.1 Introduction	23
18.2 Scope	23
18.3 Purpose.....	23
18.4 Application	23
18.5 Policy Statement	23
18.6 Guidelines	23
18.7 Enforcement	24
19.0 POLICY IMPLEMENTATION.....	24
19.1 Implementation Date	24
19.2 Monitoring and Evaluation	24
19.3 Policy Review	24
APPENDIX 1: EMPLOYEE ACKNOWLEDGEMENT.....	25
APPROVAL	26

PREFACE

On behalf of the Kenya Medical Training College (KMTc) Board, I am delighted to approve this Policy for use by Management. The KMTc Board is determined to improve access to and equity of quality medical training and to ensure that the institution plays its role in the realization of Sustainable Development Goals, Vision 2030, health sector policies and the government agenda on the “Big Four”. The Board continues to play its role in realizing the set milestones which contribute to improving the quality and quantity of essential health care providers. Inadequate numbers of skilled care providers have had a negative impact on efforts to expand access and improve the quality of health services. This situation is compounded by continued high prevalence of communicable and non-communicable killer diseases in the country.

Towards this end, the KMTc Board of Directors under my leadership is determined to critically address the task of defining long-term strategies for addressing the constraints to training and development of quality health care providers through:

- i. Improved policy and corporate governance for enhancing accountability and decision making.
- ii. Enhanced access, quality, relevance and equality in medical training.
- iii. Prudent resource utilization and good infrastructural management.
- iv. Increased visibility of Kenya Medical Training College nationally and internationally as a premier medical training institution focusing on training, research and consultancy.
- v. Improved resource base, partnership and linkages.

In response to the 2010 Constitutional agenda, the Board will continue to direct efforts at advancing community – oriented programs that respond positively to the country’s social and economic development agenda.

This Policy therefore provides an analysis of the internal and external environment, and makes strong statement on the role KMTc will play in supporting the Government realize sustainable growth in the health sector. The Board is dedicated to offer oversight on the operations and management of the College to ensure sustainable delivery of health coverage in the country and beyond. I believe successful implementation of the Policy will be realized through total commitment of the entire staff, students and other key stakeholders.



Prof Philip Kaloki, MBS,

Chairman, KMTc Board of Directors.

FOREWORD

One of the goals of Kenya's Vision 2030 in ICT is to 'Improve Kenya's competitiveness by providing timely information and delivery of government services.

This ICT Policy document is an expression of our unwavering commitment to improve the quality of services and training in KMTC through the use of ICT, as stated in the national Vision 2030 document.

The ICT Policy outlines measures that ensure an environment that encourages productivity, trust and security. It also promotes information sharing, transparency and accountability within KMTC, therefore ensuring improved services to the public at large.

This document seeks to help all staff and contractors within KMTC to adapt to new circumstances and challenges posed by emerging technologies in ICT. One of our key objectives being to strengthen internal processes through integration of ICT in the management of College operations including student services, this Policy seeks to guide developers, users of information and ICT resources on appropriate standards to be adopted at the College.

I wish to pledge the commitment of the KMTC Management in supporting and ensuring this ICT Policy is adhered to. We call upon all our staff, stakeholders and collaborators to support and cooperate with us towards achieving this goal.



Prof. Michael Kiptoo,

Chief Executive Officer.

DEFINITION OF TERMS

Server:	A computer or device on a network that manages network resources. There are many different types of servers e.g. File, Print, Database etc.
Source code:	This refers to the “before” and “after” versions of a computer program that is compiled before it is ready to run in a computer.
Protocol:	Is the special set of rules that end points in a telecommunication connection use when they communicate. Protocols specify interactions between the communicating entities.
Viruses:	A computer virus is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs.
Worms:	Is a self-replicating virus that does not alter files but resides in active memory and duplicates itself.
Trojan horse:	Is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk.
Spyware:	Is software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer’s consent, or that asserts control over a computer without the consumer’s knowledge.
Malware:	Short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems
Firewall:	Is a software or hardware-based network security system that controls the incoming and outgoing network traffic based on applied rule set.
Web:	The World Wide Web (abbreviated as WWW commonly known as the web) is a system of interlinked hypertext documents that run on and are accessed via the Internet.

ABBREVIATIONS

AMS	Academic Management System
AP	Access Point
CCTV	Closed-Circuit Television
CD	Compact Disk
DMZ	Demilitarized Zone
DNS	Domain Name Server
DSL	Digital Subscriber Line
DVD	Digital Video Disc
FTP	File Transfer Protocol
GIF	Graphics Interchange Format
HoD	Head of Department
HR	Human Resource
ICT	Information and Communication Technology
ID	Identity
ISDN	Integrated Services for Digital Network
IT	Information Technology
IP	Internet Protocol
IPPD	Integrated Payroll and Personnel Database
IPS	Intrusion Detection Systems
IPSec	Internet Protocol Security
KMTC	Kenya Medical Training College
OS	Operating System
PC	Personal Computer
PDA	Personal Digital Assistant
QoS	Quality of Service
RFP	Request for Proposal
SAN	Storage Area Network
SSh	Secure Shell
UPS	Uninterrupted Power Supply
VPN	Virtual Private Network

VISION

A model institution in the training and development of competent health professionals

MISSION

To produce competent health professionals through training and research, and provide consultancy services.

MOTTO

Training for better health

CORE VALUES

Accountability

Integrity

Responsiveness

Equity Teamwork

Professionalism

Creativity and innovation

1.0 INTRODUCTION

1.1 Preamble

One of our key objectives is to strengthen internal processes through integration of ICT in the management of College operations including student services. To achieve this, we require a concise plan of action and commitment from all concerned including students, staff and management. It is for this reason that the College has undertaken to develop a policy guideline that will serve as markers in the development, implementation and effective use of the ICT facilities at the College.

This policy will serve, alongside other related published documents, as the reference document on ICT standards.

Information and communication are integral to human society. ICT technologies have become central to modern societies, affecting all aspects of modern life. More recent technological innovations have increased further the reach and speed of communication, culminating, for now, with digital technology. These new ICTs can be grouped into three broad categories namely Information Technology, Telecommunications Technology and Networking Technology.

1.2 Statement of Purpose

This Policy seeks to guide developers, users of information and ICT resources on appropriate standards to be adopted at the College.

1.3 Objectives

- (i) To provide a framework for development and management of ICT network services that shall ensure the availability, enhanced performance and reduce the cost of running the ICT infrastructure;
- (ii) To provide guidance in developing a comprehensive, reliable and secure communications infrastructure conforming to recognized International standards supporting all services in line with the priorities of the College;
- (iii) To establish information and implement security requirements across the College's ICT infrastructure;
- (iv) To uphold the integrity and image of the College by using defined standards and guidelines to ensure the content of the College website is accurate, consistent and up-to-date;
- (v) To establish prudent practices on Internet and the College Intranet use;
- (vi) To guide the process of enhancing user utilization of ICT resources through training;
- (vii) To outline the rules and guidelines that ensure users' computers and other hardware are in serviceable order, specifying best practices and approaches for preventing failure;
- (viii) Promote information sharing, transparency, accountability and reduce bureaucracy within KMTC, and the public at large;
- (ix) To inform departments carrying out projects financed in whole or in part by the College, of the arrangements to be made in procuring ICT goods and services for the projects.

1.4 Scope

- This Policy applies to all offices and users of applications and IT systems within KMTC. It applies across hardware platforms, to all departments, KMTC Campuses, students, staff and other stakeholders.
- This Policy document covers various areas of KMTC ICT ecosystem which includes:
 - i. Passwords
 - ii. Malware
 - iii. Physical security
 - iv. Logical security
 - v. Back-up of data and information
 - vi. Email
 - vii. Internet
 - viii. Software acquisition, deployment and use
 - ix. Maintenance and support
 - x. Network development, deployment and use
 - xi. ICT training
 - xii. ICT governance
 - xiii. Acquisition, use and disposal of ict equipment
 - xiv. Website
 - xv. Computer laboratory use and security
 - xvi. Social media
 - xvii. Disaster recovery

1.5 Enforcement

KMTC will set up a structure for ongoing monitoring of compliance with this ICT Policy. The primary objective of such continuous monitoring is to identify weaknesses in the Policy framework and plug the same.

The Policy is guided by the existing Laws and Regulations which include Constitution of Kenya 2010, KMTC Act 1990 (as amended), Government ICT Standards, National environment Management Authority (NEMA), Copyright ACT of Kenya, Kenya Electronic Communication Act [2012], Public Procurement & Disposal Act and other relevant regulations currently in force.

Non-compliance to the policies and any future releases will be dealt with according to the KMTC Human Resource policies. All staff will be required to sign the Policy acceptance form signifying acceptance of this Policy in its entirety. Sanctions for non-compliance may include but not limited to the following:

- i. Temporary or permanent revocation of access to some or all computing and networking resources and facilities
- ii. Disciplinary action according to KMTC rules and regulations
- iii. Legal action according to applicable laws and contractual agreements

2.0 PASSWORD

2.1 Introduction

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of KMTC's entire corporate network. As such, all KMTC employees, contractors and vendors with access to KMTC systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.2 Scope

This Policy covers access to systems and devices both at Headquarters and Constituent Campuses.

2.3 Application

This Policy applies to system administrators, end users and contractors.

2.4 Purpose

The purpose of this Policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

2.5 Policy Statements

- i. All staff are responsible for safeguarding their system access login and password credentials and must comply with password parameters and standards identified in this policy.
- ii. Passwords must meet the complexity requirement outlined and must not be shared with or made available to anyone in any manner that is not consistent with this policy.
- iii. All user level passwords will be changed at least after three (3) months. User level passwords are for access to services such as email, website, intranet, extranet, applications, laptop and desktop computers.
- iv. System level passwords shall be changed at least once every month. System level passwords are for support of the ICT services such as root for servers, applications and networks.

2.6 Guidelines

The following are guidelines on passwords:

- a) All end users will be assigned user names and passwords by the system administrator for access to KMTC resources.
- b) ICT staff will be assigned passwords that provide them access to privileges necessary for the satisfactory delivery of their duties.
- c) In case of change job roles, the privilege access rights will be adjusted accordingly.
- d) All new KMTC staff shall only be issued with access passwords after a written request by the respective immediate supervisor.
- e) Upon receipt of a written request from the supervisor, the Head, ICT Section will delegate the creation of the required user account for the new staff by ensuring that:
 - i. Each user completes the correct user access form for each system that they need to use.

- ii. The form must identify the work role of the user in order to inform the appropriate access to the systems.
- iii. Where there is doubt about the appropriate access or role, ICT must refer to the line manager for clarity.
- f) Head of ICT shall authorize temporary disabling/removal of a user account, on receipt of a written request from Head of Human Resource Section.
- g) Passwords should not be written down, recorded/stored in any other medium unless the said storage is itself encrypted.
- h) No passwords for any system may be stored or transmitted in clear text.
- i) Users are prohibited from sharing their personal passwords to other people whether KMTC staff or not.
- j) Users shall not use the 'Remember password' feature for any application whether web based or not.
- k) Where there is suspicion that a password has been compromised, the user should consult ICT for appropriate corrective action.
- l) Maximum number of user login attempts shall be restricted to three (3) after which the password will lock.
- m) All computers or laptops connected to the KMTC network resources should lock within ten (10) minutes of unattended time.
- n) All passwords shall not be less than eight (8) characters and shall be of a combination of alpha numeric and special characters.

2.7 Enforcement

Loss or damage to College data emanating from breach of this Policy guideline will subject the user to appropriate disciplinary action.

3.0 MALWARE

3.1 Introduction

A major threat to the delivery of ICT services is malicious software which has the potential to undermine the confidentiality, integrity and availability of those services/data hosted on ICT systems.

3.2 Purpose

The purpose of this Policy is to protect KMTC resources and data against the threat of malware. It provides guidance and direction on minimizing the risk of a malware infection(s) and what to do if one is encountered.

3.3 Scope

This Policy covers computer systems and communication networks.

3.4 Application

This Policy applies to staff and students authorised to use/access those computer systems and communication networks.

3.5 Policy Statement

Head ICT will ensure that appropriate technical measures are implemented to protect against malware and to ensure that appropriate controls are in place to rapidly detect, isolate and remove any instances.

3.6 Guidelines

Recommended processes to prevent virus problems:

- a) All computers or any other external data storage device (whether official or owned by the individual) that are connected to the KMTC network shall be scanned using a standard corporate antivirus.
- b) All access devices such as computers connected to KMTC network shall be running an approved anti-virus.
- c) KMTC shall make sure that there is availability of an approved KMTC anti-virus at any point in time.
- d) Regular updates of the anti-virus in use will be maintained.
- e) Users shall immediately inform the ICT department once virus infection is suspected.
- f) All infected computers or other devices connected to KMTC network found to have been infected by virus (es) should be disconnected immediately until proof of disinfection is provided. Users will be made aware of the problem of hoaxes and the action to be taken on receipt thereof.
- g) Users shall not open email attachments that are from suspicious sources. If not sure, either destroy the email or bring it to the attention of ICT staff.
- h) Users shall not download files from unknown or suspicious sources.
- i) Users shall not visit suspicious sites such as those that promise you to click and win and X-rated sites.
- j) Users shall avoid direct disk sharing and at all times run a scan on every removable disk to avoid malware.

3.7 Enforcement

Any employee found to have violated this Policy shall be subjected to disciplinary action in line with the Human Resource Manual.

4.0 PHYSICAL SECURITY

4.1 Introduction

Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism.

4.2 Scope

This Policy covers all organizational ICT facilities, equipment, cabling and end user devices.

4.3 Application

This Policy applies to ICT staff, contractors, vendors and students.

4.4 Purpose

This Policy is intended to ensure that physical computer and information resources are properly protected.

4.5 Policy Statement

The College will ensure that access to specific areas restricted to those who are assigned access privileges and that all equipment is well marked and protected.

4.6 Guidelines

- i. The server room or any other critical ICT facility shall remain out of bounds to all people except authorized staff. In cases where there is justified request to access these areas, written authorization should be sought from the Head of ICT.
- ii. Where access is by people other than the authorized ICT personnel, name, reason of visit, the day and time of access shall be logged in a register and the visitor should be accompanied by an authorized ICT staff.
- iii. All computers shall be connected to the power through a UPS. The server class computers and other critical equipment shall also be connected to surge protectors
- iv. All ICT staff, consultants, vendors, visitors etc. shall wear identification badges at all times.
- v. All instances of entry and usage of equipment in the server room shall be registered in a log file.
- vi. Emergency access rights to systems for maintenance purposes shall only be approved by the Head of ICT.
- vii. All servers or network active equipment shall be kept locked up at all times and access to them will be logged.
- viii. All windows or openings which are in high-risk zones shall be protected using metal grills.
- ix. The server room shall have access control system and where possible CCTV cameras installed.
- x. The server room floor shall be raised (probably a false floor) to protect the interconnecting cables, plugs and power connectors.
- xi. Users shall not bring into the server room food or liquid of any kind unless the liquid is for setup or maintenance purposes in the server room.
- xii. There shall be fire extinguishers placed conveniently next to critical ICT resource areas.
- xiii. There shall be a fire detection and suppression system in the server room.
- xiv. The Air conditioning system shall be designed to provide required temperature and humidity condition recommended by the manufacturers of the servers to be installed within the server room.
- xv. Access to media and manuals such as tape, disk, and documentation libraries shall be restricted exclusively to those staff whose responsibility is the maintenance of those libraries.

- xvi. Head of ICT has authority to permit off site removal of ICT assets to the staff and non-staff.

The time limit, and purpose of the removal will be recorded and returns verified for compliance.

- xvii. Equipment and media taken off premises shall not be left unattended in public places.
- xviii. Manufacturers' instructions for protecting equipment shall be observed at all times. No loads shall be placed on computers, network cables or any other ICT equipment.
- xix. No drainage pipes shall run within or above computer server rooms to reduce the risk of flooding.
- xx. ICT Section shall be notified of works to be carried out at least 24 hours in advance of its commencement.
- xxi. All KMTC Computer hardware shall be prominently marked, either by branding or etching, with the name of the Department / Office or computer laboratory where the equipment is normally located.
- xxii. Power feeds to the servers shall be connected through Uninterrupted Power Supply (UPS) and surge protector equipment to allow the smooth shutdown and protection of computer systems in case of power failure.
- xxiii. Where possible generator power shall be provided to the computer suite to help protect the computer systems in the case of a mains power failure.

4.7 Enforcement

Violation of this Policy may be subject to disciplinary action up to and including denial of access, legal penalties, and/or dismissal in line with the HR manual. Any employee aware of any violation of this Policy is required to report it to their supervisor or other authorized representative.

5.0 LOGICAL SECURITY

5.1 Introduction

Logical security consists of software safeguards for an organizational systems, including user identification and password access, authenticating, access rights and authority levels.

5.2 Scope

This Policy covers logical access to all KMTC systems and applications to protect the privacy, security, and confidentiality of KMTC systems, especially highly sensitive systems, and the responsibilities of institutional units and individuals for such systems.

5.3 Application

This Policy applies to staff and students with access to KMTC systems and applications.

5.4 Purpose

Logical security measures are meant to ensure that only authorized users are able to perform action or access information in a network or a workstation.

5.5 Policy statement

The College will ensure that access to specific information or data is restricted to those who are assigned access privileges.

5.6 Guidelines

- i. ICT Section shall ensure that audit logs are monitored and any exceptions are investigated.
- ii. Users are required to shut down their workstations at the end of the day.
- iii. ICT Section will ensure that information is accessed in line with data classification scheme as per the Records Management Policy.
- iv. Users shall remain responsible for all activities performed under their profile by strictly observing the password Policy.
- v. The System Administrator and the Database Administrator should not be able to alter their own activity log files.
- vi. Only authorized users of the College ICT services shall be granted access to remote connections. However the following are binding:
 - a) The prevailing procedures on usage of the College ICT resources will remain in force during the remote access session
 - b) The session shall be logged in a register
 - c) The user shall ensure that the security of the College ICT services are not affected by their activities
- vii. The College will conduct a risk assessment as per prevailing procedures to determine the level of monitoring required for a specific application or system, taking the following into consideration:
 - a) Criticality of the application processes;
 - b) Value, sensitivity and criticality of the information involved as defined by the Information Classification and Handling Procedure;
 - c) Past experiences of system infiltration and misuse, and the frequency of vulnerabilities being exploited;
 - d) Extent of system interconnection;
 - e) Disabled logging facilities.
- viii. All KMTC internet gateways shall have firewalls and Intrusion Detection Systems (IDS) installed and running.
- ix. KMTC shall have host based IDS installed in its server class computers.
- x. User access privileges on a server shall be allocated on “least possible required privilege” terms, just sufficient privilege for one to access or perform the desired function.
- xi. Super-user accounts such as “root” shall not be used when a non-privileged account can do.
- xii. If a methodology for secure channel connection is available, that is technically feasible, privileged access shall be performed over secure channels, for instance, encrypted network connections using SSH or IPsec.

5.7 Enforcement

Logical security is critical for protecting the security of the organization, employees that purposely violate this Policy may be subject to disciplinary action in line with the HR policies. Any employee aware of any violation of this Policy is required to report it to their supervisor or other authorized representative.

6.0 BACK-UP OF DATA AND INFORMATION

6.1 Introduction

Backups ensure business continuity in case of a disaster. Data custodians are responsible for providing adequate backups to ensure the recovery of data and systems in the event of failure. These backup provisions will allow Organization business processes to be resumed in a reasonable amount of time with minimal loss of data. Since hardware and software failures can take many forms, and may occur over time, multiple generations of institutional data backups should be maintained.

6.2 Purpose

The purpose of this Policy is to preserve the confidentiality, integrity, and availability of the College data and information.

6.3 Scope

This Policy addresses backup and restore aspects of College data and information

6.4 Application

This Policy is applicable to Database Designers/Administrators, System & Network Administrators, contractors, service providers and consultants.

6.5 Policy Statement

The Head ICT will ensure that College data and information is back up regularly.

6.6 Guidelines

- i. All information systems shall have both onsite and offsite backups performed on them.
- ii. Offsite backups shall be done at least once a month
- iii. All configuration settings for servers and network equipment shall be backed up.
- iv. All backup files shall be kept in a secure location from effects of fire, water, theft or any other risk.
- v. All backups shall be recorded in the backup register, which should have the following details:
 - a) Date the backup was carried
 - b) Database/system backed up
 - c) Person who did the back up
 - d) Time the backup was performed
- vi. All onsite backup files shall be stored away from the rooms in which the system being backed up exists.

- vii. The backup media shall be labeled appropriately, indicating the type of backup and the schedule
- viii. Access to backup media and its contents shall only be given to authorized personnel
- ix. All software installations shall have backup of the configuration immediately after deployment. Regular backups of the software shall be done after every two quarters
- x. Disposal of backed up data shall be guided by the prevailing Information Security policy in place at the time.
- xi. Backups shall be tested every three (3) months to ensure they are working
- xii. The testing shall be done on “test beds”, as testing on the “live” systems may lead to undesirable results.
 - a) The College shall create shared data folders for users to backup critical and reference files for different user groups.
 - b) All system owners of the information systems in the College shall liaise with the ICT Section to formulate appropriate data backup plans for their systems
 - c) All security-related events on critical or sensitive systems shall be logged and audit trails backed-up in all scheduled system backups.

6.7 Enforcement

Any user found to have violated this Policy may be subjected to disciplinary action as per the College’s disciplinary procedures.

7.0 EMAIL

7.1 Introduction

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

It is important to note that the emails services are key communications tool in the College. Inappropriate use of the email system can lead to malware infection, which ultimately could lead to degradation of network performance and in extreme circumstances crush the entire KMTC system.

7.2 Scope

The Policy addresses usage of email in the College.

7.3 Application

This Policy applies to all KMTC staff and students.

7.4 Purpose

The College must be able to communicate quickly and efficiently with employees and stakeholders in order to conduct official College business.

E-mail is an appropriate medium for such communication and supports KMTC goals regarding cost efficiency, expediency, and sustainability.

This Policy is not intended to limit the use of other communication tools.

7.5 Policy Statement

It is the Policy of KMTC that the staff E-mail system is an appropriate medium for official communications from the College to the employees, stakeholders and other third parties. It is the responsibility of College staff to receive such communications and to respond to them as may be necessary.

7.6 Guidelines to Acceptable E-mail use

- i. All electronic mail (emails) will be centrally available the Headquarters.
- ii. Users will be granted email accounts once an official request has been made through the immediate supervisor to the Head ICT.
- iii. Email account access will cease on exit of staff from service at the College.
- iv. When using the email or messaging system, users must at all times respect the privacy and personal rights of others
- v. Staff are prohibited from knowingly transmitting emails that contain virus-infested attachments.
- vi. Staff shall make sure the computer (if it is a personal one) they are using to access the email has up-to-date anti-virus running.
- vii. Users shall not transmit confidential data and information through email.
- viii. Staff shall not transmit abusive material, pornography, insensitive data or information, copy righted material or junk mail.
- ix. Users shall not use e-mail for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses).
- x. The College prohibits personal use of its e-mail systems and services for unsolicited mass mailings, non-KMTC commercial activity, political campaigning, dissemination of chain letters, and use by non-employees.

7.7 Enforcement

The head of ICT shall ensure compliance with this Policy through continuous monitoring.

Contravention of this Policy may lead to disciplinary measures such as temporary suspension or permanent closure of the user's email account, or other disciplinary measures as guided by the KMTC disciplinary procedures.

8.0 INTERNET

8.1 Introduction

The Policy provides employees with rules and guidelines about the appropriate use of KMTC equipment, network and Internet access. It helps to protect both the College and the employee; the employee will be aware that browsing certain sites or downloading files is prohibited and that the Policy must be adhered to or there could be serious repercussions, thus leading to fewer security risks for the College as a result of employee negligence.

8.2 Purpose

The purpose of the Policy is to define the appropriate use of the internet by KMTC employees, students and stakeholders.

8.3 Scope

This Policy covers internet usage at KMTC.

8.4 Application

The internet usage applies to all internet users who access the internet through the computing or networking resources.

8.5 Policy Statement

The Policy provides employees with rules and guidelines about the appropriate use of KMTC equipment, network and Internet access.

8.6 Guidelines

- i. Staff are required to responsibly use Internet when granted access.
- ii. Account details such as passwords shall be maintained as indicated in the Password Policy.
- iii. The data sent through Internet should be considered “public” and therefore shall be encrypted to minimize risk.
- iv. Copyrighted material should not be distributed, copied or published in any form without the written permission from the originator.
- v. The liability for any copyright violation or infringement rests solely on the user/employee.
- vi. Download and installation of any software in the College devices should be done by ICT staff.
- vii. Non ICT staff who want to install software should seek prior authorization from the Head ICT or a delegated authority.
- viii. Internet service should not be used for personal business of any kind including consultancies.
- ix. Staff or any other user has no rights of privacy in their use of the Internet service provided by the College.
- x. A user is prohibited from the following activities :
 - a. Distributing of unsolicited advertising, junk mail or chain letters;
 - b. Sending or receiving sexually oriented messages or images;
 - c. Visiting derogatory or racially intolerant websites;
 - d. Visiting sites for personal entertainment;
 - e. Soliciting money or advocating a religious or political cause;
 - f. Use of abusive, vulgar, or objectionable language in the course of the Internet usage;
 - g. Transmitting of any type or quantity of data that may cause disruption of services to others;
 - h. Propagating computer worms, viruses or other potentially malicious code;
 - i. Unauthorized entry to other computer or network resources.
- xi. Networking services, resources or facilities should not be used for any purposes that violate any existing laws, regulations, policies or procedures whether external or internal.

- xii. All Internet access software shall be configured to use stipulated gateways, firewalls, or proxy servers. Bypassing any of these servers shall be strictly prohibited.
- xiii. Internet access traffic through the KMTC ICT infrastructure shall be subject to logging and review.

8.7 Compliance

Head of ICT shall monitor and audit Internet access for the purposes of assuring system security, proper usage, and for impact on performance.

Illegal usage will be solely attributed to the staff concerned and will warrant disciplinary actions

9.0 SOFTWARE ACQUISITION, DEPLOYMENT AND USE

9.1 Introduction

Software is one of the three major components of any information system. The other two components are hardware and users. The College has identified several areas that need automation as a way of improving service delivery. A large component of any automation would need acquisition of software.

9.2 Purpose

The purpose of this Policy is to provide guidance on appropriate processes and criteria for acquisition, deployment and use of software in any KMTC device. It seeks to minimize loss of desired software functionality; the exposure of sensitive information in KMTC's computing resources and the risk of malware & legal exposure of running unlicensed software.

9.3 Scope

This Policy covers all software whether free and Open Source Software, proprietary or any other type in use in KMTC computing resources.

9.4 Application

This Policy applies to all KMTC staff, students and stakeholders.

9.5 Policy Statement

The Policy provides employees with rules and guidelines about the appropriate acquisition, development and use of software in KMTC.

9.6 Guidelines

- i. As a rule, KMTC shall always evaluate the capacity of developing its software in-house. This shall be weighed against other feasibility factors such duration, cost, other ongoing projects, etc. Thereafter, KMTC will explore Free and Open Source Software (FOSS) before settling on purchase.
- ii. A preliminary feasibility study findings document shall form part of the proposals for software acquisition submitted for consideration

- iii. All major software acquisition projects shall have a project implementation team with a project manager/implementation coordinator. The team shall comprise representatives from the user department, ICT department, Administration, Finance, Procurement, Human Resource departments and any other members appointed by the Director / CEO.
- iv. In cases where the software is customized FOSS, in-house developed, outsourced developed, the adopted institutional software development methodology at the time shall be used.
- v. All software/patches/upgrades shall be tested in a development environment using dummy and live data before installation. The user representative with the help of ICT Section shall sign a system compliance document validating the test results.
- vi. All software or pieces of software developed using KMTC ICT services in the course of employment at KMTC shall remain the property of KMTC.
- vii. The College shall ensure that it attains the maximum level of integration of its MIS applications. To achieve this, the College will perform an ICT needs assessment to determine the best way of doing it.
- viii. All MIS applications shall have a user representative who will be responsible for articulating the needs of the user group in terms of acquisition, deployment, training, upgrading and maintenance.
- ix. All MIS acquisitions shall have a project proposal submitted to the ICT Steering Committee for vetting before approval for acquisition is sought from the CEO.
- x. All MIS applications shall be required to have the following manuals both in soft and hard copy:
 - a. End User Manual
 - b. Operator Manual
 - c. System Administration Manual
- xi. All MIS applications shall have an in-built user help system.
- xii. Training shall be conducted for end users and technical staff.
- xiii. For all outsourced MIS solutions, there shall be a Service Level Agreement (SLA) signed between the vendor and the College for continuous online support for the MIS.
- xiv. For all outsourced MIS solutions, there shall be a source code escrow agreement.
- xv. Any outsourced MIS solutions shall be handed over to the College after implementation.
- xvi. For the internally developed applications, the College shall ensure that enough capacity is build both at end user and technical level for the long sustainability of the application.
- xvii. All in-house developed software must have inline documentation of the source code.
- xviii. All requests by users who do not fall in the functional domain of the particular MIS shall be channeled through the Head of ICT.
- xix. KMTC shall ensure Licenses for commercial software are provided upon acquisition, duly registered and subsequently renewed as per the requirements of the copyright.

9.7 Enforcement

Contravention of this Policy may lead to internal disciplinary action as per the KMTC disciplinary procedure, or face criminal proceedings as per the law.

10.0 MAINTENANCE AND SUPPORT

10.1 Introduction

The primary mission of the ICT service desk is the support of College's hardware and software. This includes but not limited to; desktop computers, printers, laptops, hand-held computing devices, and peripheral devices such as scanners, zip drives, and modems.

A team of experienced technical staff will work with the staff members to ensure that their computer equipment is properly maintained and performing reliably to provide the support services described in this policy.

10.2 Purpose

The purpose of this Policy is to ensure that the ICT service desk approach is to take a proactive role and work with staff to make sure that the ICT equipment purchased by the College is properly maintained to function reliably for its expected life span.

An important part of this approach is to work with departments to plan for a realistic replacement cycle to eliminate unreliable and obsolete equipment.

10.3 Scope

This Policy addresses maintenance and support of the College ICT devices, Software and services.

10.4 Application

This Policy applies to all KMTC staff and students

10.5 Policy Statement

This Policy provides guidance on maintenance and support for all ICT related equipment and facilities in use at the College.

10.6 Guidelines

In an effort to ensure sustainability of ICT services provided to users, the College seeks to offer necessary support and maintenance services.

- i. All hardware and software purchased shall be covered either by warranty or by an Annual Maintenance Contract (AMC).
- ii. KMTC shall adopt and customize a mature and established ICT service delivery methodology to guide the College in support and maintenance of its ICT services.
- iii. All computers or hard disks having a fresh installation or moved from other networks/ computers shall first be scanned before installation.
- iv. An annual maintenance work plan shall be developed, incorporating the manufacturer's recommendations, and an associated budget developed, implemented and reviewed by ICT Section.
- v. All contractors working in high security zones such as Network Operations Centers (NOCs), data centers and server rooms shall have accompanied supervision.
- vi. Where maintenance of equipment requires shipping the equipment outside KMTC premises, any sensitive data shall be backed up and erased through a suitable method. Where data cannot be erased, a Non-Disclosure Agreement shall be signed by the vendor.

- vii. KMTC shall maintain an online Service Desk help system and once in place, users will be required to use the system as the first option of reporting incidences or making other requests.
- viii. The College shall setup a maintenance workspace for handling minor maintenance duties.
- ix. Where not possible for ICT Section to sort out an incidence, hardware or otherwise, it shall be referred to a vendor.
- x. ICT Section and by extension the College is not responsible for support or maintenance of privately owned hardware or software.
- xi. ICT Section is responsible for advising and giving direction to all ICT related projects or activities in KMTC.
- xii. It shall be the duty of ICT department to format user requirements in a language and format understandable by vendors, developers and other technical persons through appropriate specifications.
- xiii. There shall be an annual ICT services satisfaction survey conducted whose findings will inform planning for future activities.
- xiv. It shall be the duty of the users to provide requirements/ features of the hardware or software that they wish to have procured.
- xv. The ICT Section shall be responsible for the maintenance activities related to the system such as patches and upgrades in collaboration with the user department.
- xvi. The ICT Section will only support KMTC Licensed Software and expressly forbids the installation of the following softwares:
 - a) Privately owned software
 - b) Pirated copies of any software
 - c) Any software not installed according to the procedures set out in this Policy

10.7 Enforcement

The head of ICT shall ensure compliance with this Policy through continuous monitoring.

Contravention of this Policy may lead to disciplinary measures such as temporary suspension or permanent closure of the user's email account, or other disciplinary measures as guided by the KMTC disciplinary procedures.

11.0 NETWORK DEVELOPMENT, DEPLOYMENT AND USE

11.1 Introduction

All network links will be centrally administered from the HQs and the design of the links will be considered under the prevailing conditions such as finance, technology and user needs at the time.

11.2 Purpose

This Policy seeks to establish the responsibility and authority for ownership, acquisition, and management of the College enterprise network infrastructure.

11.3 Scope

This Policy covers network infrastructure at KMTC.

11.4 Application

This Policy applies to all KMTC Staff and contractors.

11.5 Policy Statements

- This Policy must support different sets of business needs at diverse locations throughout the College.
- The Policy is meant to ensure consistency in the network architecture and to ensure the network meets National ICT network standards.

11.6 Guidelines

The following guidelines will support the network development, deployment and usage:

- i. The ICT strategy shall take into consideration the necessary resources to support the network needs of the users.
- ii. All active device connections to KMTC network shall be approved by the Head of ICT.
- iii. No active equipment or private networks in KMTC shall be installed without the written authority of the Head of ICT.
- iv. All systems or devices connected to the internet, through broadband modem shall be disconnected from KMTC Local Area Network (LAN) or Wide Area Network (WAN).
- v. KMTC staff who want to connect privately owned computers or other device to KMTC network will only do so after ICT Section is assured that the connection of the said device will not lead to denial or degradation of service to other users.
- vi. All KMTC ICT Networks shall conform to Government ICT Network Standards.

11.7 Enforcement

ICT staff will carry out regular network audit and inspection exercises. Misuse of the network resources may lead to suspension or termination of access rights to the network. For minor incidences, the Head ICT may take action and inform the Management while for the serious incidences, the matter will be referred to the ICT Steering Committee for action.

12.0 ICT TRAINING

12.1 Introduction

A computer literate user base complimented by well-trained ICT staff is the best combination for effective service delivery. In view of this, the College emphasis on ICT training shall be on two fronts:

- i. End user training
- ii. ICT staff training

12.2 Purpose

The purpose of this Policy is to continuously identify the ICT training needs and prepare a training program for adoption and execution by the College Training Committee.

12.3 Scope

This Policy covers ICT training for KMTC Staff.

12.4 Application

This Policy applies to the ICT staff and end users.

12.5 Guidelines

- a) The ICT department shall continuously identify the training needs to ensure that a measure of ICT needed skills is done through an annual Training Needs Assessment. The recommendations of this assessment shall be implemented through HR Training Committee.
- b) The College shall ensure existing staff have basic computer proficiency skills .

13.0 ICT GOVERNANCE

13.1 Introduction

The importance of control and management of business process in success of an organization cannot be gainsaid. While procurement of services is essential for the growth of an organization, it is even more important to have the necessary governance structures and staff capacity to support those services.

13.2 Purpose

The purpose of the ICT governance Policy is to give the institution clear and concise direction in managing the use of ICT. This will allow the College to give strategic direction, monitor services, mitigate internal and external risks and ensure objectives are achieved.

13.3 Scope

This Policy focuses on ICT structure and governance.

13.4 Application

This Policy applies to the Board of Directors and KMTC Management.

13.5 Guidelines

- i. The College shall ensure that there is enough ICT skills to manage ICT services in the following major areas:
 - a) ICT management
 - b) ICT infrastructure management and maintenance
 - c) Local and wide area network administration and maintenance
 - d) Systems administration skills
 - e) Applications development, maintenance and management
 - f) Security and audit
- ii. KMTC shall setup an ICT Steering Committee to provide oversight matters to issues related to ICT.

- iii. KMTC shall develop and implement an ICT strategy that is aligned to the Institutional Strategic plan.

13.6 Compliance

The College Board of Directors and Management shall ensure compliance with this Policy.

14.0 ACQUISITION, USE & DISPOSAL OF ICT EQUIPMENT

14.1 Introduction

Policy and guidelines for the acquisition of computing hardware has been set in order to facilitate ICT asset management and inventory tracking of the College's technology. The procedures set forth in this Policy will ensure technology acquisition adhere to minimum Government standards for hardware.

14.2 Purpose

This Policy governs the acquisition, use and disposal of hardware within the College.

14.3 Scope

This Policy addresses the acquisition, use and disposal of all ICT equipment.

14.4 Application

This Policy applies to ICT Staff, Supply Chain Management Staff and KMTC Management.

14.5 Policy Statement

All ICT equipment procured shall meet the approved minimum technical specifications. The use and disposal of such hardware shall be as stipulated in this Policy.

14.6 Guidelines

- i. All requests for ICT equipment must be recommended by the ICT Section.
- ii. All hardware acquired by the College must meet the requirements of the Government ICT standards.
- iii. Manufacturer's instructions on use of equipment shall be observed at all times.
- iv. All network active equipment, computers, servers and laptops shall be comprehensively insured.
- v. Where computers, hard disks or any other media of data storage is being disposed, the data shall be totally erased to unrecoverable state.
- vi. ICT Section shall recommend disposal of all obsolete hardware based on the manufacturer's recommendations.
- vii. Hardware assets must be checked prior to disposal to ensure that any KMTC record have been included in a KMTC record keeping system.
- viii. Hardware assets to be disposed of externally must be handled using the approved procedures. The entity performing the service must certify that each item has been disposed of securely and in compliance with environmental guidelines.

14.7 Enforcement

- KMTC users are responsible for the care of the hardware assigned to them. Should the loss or damage of the hardware be attributable to negligence on the part of the user he/she will incur costs related to the repair or replacement of the equipment.
- Contravention of this policy may lead to internal disciplinary action or criminal proceedings taken against the person.

15.0 WEBSITE

15.1 Introduction

A good website is a powerful tool of promoting interaction with the outside world. It is therefore necessary for the College to put in place measures that promote its management and use to enhance its presence in the worldwide web.

15.2 Purpose

This Policy has been developed in order to streamline the Website design, development, maintenance and management to keep the quality of the website high.

15.3 Scope

This Policy applies to all Web sites owned and/or managed by KMTC.

15.4 Application

This Policy applies to all employees of KMTC, students and stakeholders.

15.5 Policy Statement

The College website aims to provide accurate, useful and timely information on all aspects of the College activities to staff, students and stakeholders.

15.6 Guidelines

- i. Design and review of the website will be done by the Website Management Committee in consultation with the relevant departments. The composition of this Committee shall be in line with Government ICT Standards.
- ii. The website design shall be such that all the web pages are viewable in standard compatible web browsers, various operating systems, devices including mobile phones and tablets.
- iii. The website shall be hosted in a secure location that conforms to Government ICT standards to protect the College from embarrassment of defaced website.
- iv. Web-based applications which access public data shall be isolated from the website and fully secured.
- v. Principals and HoDs are allowed to submit content on matters relating to their areas of operation for posting through the Corporate Communications Manager.
- vi. All Web content submitted must be approved prior to posting by the Corporate Communications Manager.
- vii. All submissions must be forwarded at least one week in advance of the requested posting date. If significant changes are required to the content, this timeframe may be extended.

- viii. Only the following file formats can be submitted for posting: .doc, .pdf or any other format agreed upon by the ICT department.
- ix. In case of copyrighted work, written permission of the copyright holder shall be produced on submission.

16.0 COMPUTER LABORATORY USE AND SECURITY

16.1 Introduction

Computer Laboratories provide space for students' learning and research activities. Each KMTC campus is required to have a computer Lab for students to access these services.

16.2 Scope

This Policy covers acceptable use of Computer Laboratories in all Campuses.

16.3 Purpose

This Policy is intended to ensure Computer Laboratories provide computer equipment in a conducive environment to help students and staff be productive.

16.4 Application

This Policy is intended for students and staff who use the computer laboratory.

16.5 Policy Statement

All students and staff who use the Computer Laboratories, shall abide by the guidelines in this Policy.

16.6 Guidelines

- a) All the KMTC campuses shall appoint officers, who shall take charge of their computer laboratories. The Principals shall formally inform the ICT department of the names and contacts of the appointed officers.
- b) Use of the computer laboratory will be subject to existing rules and regulations.
- c) No computer laboratory shall replicate the core production services offered by the ICT department. Production services shall be defined as all shared critical services running over the KMTC ICT infrastructure that generate revenue streams or provide customer capabilities.

16.7 Enforcement

Failure to follow this Policy can result in disciplinary action in accordance with Human Resources Manual. Disciplinary action for not following this Policy may include termination, as provided in the applicable handbook or employment guide.

17.0 DISASTER RECOVERY

17.1 Introduction

Disaster Recovery is the retrieval and continuation of vital technology for infrastructure and systems following a natural or human induced disaster.

17.2 Scope

The scope applies to all ICT services and managed systems in the College.

17.3 Purpose

This Policy is intended to provide guidelines to be used in developing disaster recovery plans, business contingency plans, business continuity plans and the process of recovering from a disaster.

17.4 Application

This Policy applies to all staff and especially Network Managers, System Administrators and Application Administrators who are responsible for systems or for a collection of data held either remotely on a server or on the hard disk of a computer.

17.5 Policy Statement

All critical KMTC ICT enabled services shall be restored and maintained as quickly as possible following any major disaster and failure that affects them at the College.

17.6 Guidelines

- i. A computer emergency response plan shall be created detailing who is to be contacted, when, how and what immediate actions must be taken in the event of certain occurrences.
- ii. A succession plan shall be created describing the flow of responsibility when normal staff is unavailable to perform their duties.
- iii. A data study shall be created detailing the data stored on the systems, its criticality, and its confidentiality.
- iv. Criticality of service list shall be done to list all the services provided and their order of importance. It shall explain the order of recovery in both short-term and long-term timeframes.
- v. A data backup and restoration plan shall be created detailing which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered.
- vi. Equipment replacement plan shall be created describing what equipment is required to begin to provide services, list the order in which it is necessary and note where to purchase the equipment.
- vii. Management shall set aside time to test implementation of the disaster recovery plan. Table top exercises shall be conducted annually.

17.7 Enforcement

Since proper disaster recovery planning and implementation is critical for maintaining the business functionality of the organization, employees that purposely violate this policy may be subject to disciplinary action up to and including denial of access, legal penalties, and/or dismissal. Any employee aware of any violation of this Policy is required to report it to their supervisor or other authorized representative.

18.0 SOCIAL MEDIA

18.1 Introduction

This Policy presents and explains the rules governing social media use at the College. It explains how designated staff must use the College social media accounts. It also explains the rules surrounding personal social media use during working hours and what employees may comment on KMTC and the College related issues on their personal accounts.

18.2 Scope

This Policy covers access and use of social media platform during working hours or work related activities outside the stipulated standard working hours.

18.3 Purpose

This Policy will ensure that employees, regardless of their position in KMTC, use their social media accounts in an acceptable and secure manner.

18.4 Application

This Policy applies to all KMTC staff and students.

18.5 Policy Statement

This Policy ensures appropriate access, use and management of social media.

18.6 Guidelines

- a) There shall be a designated officer to manage KMTC presence in social media platforms.
- b) The ICT administrator shall limit social media platforms in KMTC based on impact on Network bandwidth, employee productivity, potential avenue for exposure or leakage of sensitive information and potential avenue for malware.
- c) Users shall connect to and exchange information with only those social media sites authorized by Management and in accordance with other government policies.
- d) Users shall not speak on social media sites on behalf of KMTC unless specifically authorized by KMTC Management.
- e) Users shall avoid mixing their professional information with their personal information.

18.7 Enforcement

Employees who purposely violate this Policy may be subject to disciplinary action up to and including denial of access, legal penalties and/or dismissal. Any employee aware of any violation of this Policy is required to report it to their supervisor or other authorized representative.

19.0 POLICY IMPLEMENTATION

19.1 Implementation Date

This reviewed Policy takes effect on the date it is approved by the KMTC Board of Directors.

19.2 Monitoring and Evaluation

- i. The ICT Section shall conduct monitoring and evaluation of the effectiveness of this Policy in line with the Monitoring, Evaluation and Reporting framework.
- ii. The College shall:
 - a. Develop and maintain strategies and mechanisms for monitoring and evaluation of this Policy.
 - b. Undertake regular check on implementation of the Policy.
 - c. Carry out annual evaluation on the implementation of the Policy.
 - d. Use the information for planning and management.
 - e. Propose potential areas for review.

19.3 Policy Review

The Policy will be reviewed after every five (5) years or earlier if need arises with an aim to enhance efficient delivery of effective outcomes.

APPENDIX 1: EMPLOYEE ACKNOWLEDGEMENT

I have read and understand KMTC's ICT Policy. I consent to adhere to the rules outlined in the Policy. I understand that violation of any of the above Policy may result in disciplinary action including termination of employment.

Full Names

P/NO:

Station

Department

Signature

Date

APPROVAL

Title : Information and Communication Technology Policy

Contact : Deputy Director Finance and Administration

Approval Authority : The Board of Directors

Commencement Date : May 2019

SIGNED



**Prof. Philip Kaloki, MBS,
Chairman, KMTC Board of Directors.**

15th May 2019

Date



KMTC is ISO 9001:2015 Certified.

Kenya Medical Training College


PO BOX 30195-00100

Nairobi, Kenya.

Tel: 020-2725711/2/3/4

0737-352543 | 0706-541869 | 020-2081822/23

Website: www.kmtc.ac.ke

 : @Kmtc_official

 : @KMTCoifficial