KAGUMO TEACHERS' TRAINING COLLEGE

DATA, INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY, PROCEDURES AND STANDARDS MANUAL

2025

KAGUMO TEACHERS' TRAINING COLLEGE

P.O. BOX 18, 10100 NYERI

Mobile No.0701972912 (Calls only)

Mobile No. 0796632055

Email: info@kagumocollege.ac.ke

Website: www.kagumocollege.ac.ke

ISO 9001:2015 CERTIFIED

A BRIEF BACKGROUND OF THE COLLEGE

Kagumo TTC - which started as a primary school- has a long history as an institution of learning; a history that stretches back to the early years of the 20th century. The land parcels on which the College stands were acquired for institutional purposes through the intervention and mediation of the African council in 1928. However, the actual construction of the first buildings – offices for the principal – began in 1930.

The institution incorporated a primary teachers' training College in 1944 with a humble enrolment of eight (8) students and a small staff of six (6). Later, it expanded to cater for an increased demand for teachers in the country. This significant expansion was strengthened further when Kagumo became an academic complex through the introduction of a secondary school wing in 1949.

In 1982, the College underwent another significant upgrading. It started offering the Diploma in Teacher Education (DTE) curriculum whose graduates were posted to secondary schools. In this upgrading, the College was responding to the demands of the social and economic dynamics of the time. The first batch of 283 DTE trainees graduated in 1984.

The College grew successfully through the 1980s. However, due to further challenges, adjustment to the curriculum was inevitable. The year 1990 saw the phasing out of some subjects in humanities; precisely, Kiswahili, C.R.E., History and Geography. Among other reasons, this consideration was aimed at increasing the capacity of the College to train teachers in the highly needed science-based subjects. Consequently, Physics, Chemistry, Biology and Mathematics were introduced into the diploma curriculum. The aforesaid transformation was taking place while then first lot of the newly introduced 8-4-4 system of education was approaching its secondary level maturity stage with the first lot of the 8-4-4 system trainees being admitted for the DTE course in 1993.

Another concomitant consideration was the upward revision of the course duration from two (2) to three (3) years. Similarly, the duration of the teaching practice was increased to two terms taken during the final year of study. In 2022, in alignment to the Governments new education system, the first cohort of 314 students to train under the Competency-Based Curriculum was admitted.

OUR VISION, MISSION AND CORE VALUES

Our Vision

A Transformative, Self-directing and Competent Teacher

Our Mission

To provide inclusive and market-driven teacher education and training

Core Values

We commit to championing the following core values as the guiding principles in our undertakings:

God's guidance	We depend on God and recognize God as the ultimate owner of all talents, resources, and opportunities that we use on a daily basis
Integrity	We are honest, impartial and trustworthy at all times as we relate with our colleagues, customers and all stakeholders. We deliver our services in a manner which is fair and free of discrimination or preferential treatment
Professionalism	We value our work, and act in a reliable manner that depicts our expertise and competences. We deliver as a team and take great pride in our accomplishments
Innovation & Creativity	We promote accessibility and affordability, seek new and more effective approaches to education, while exercising creativity as we chart inventive paths into the future
Team Work	We foster teamwork by creating a culture that values collaboration and seeks out different perspectives. We value the significant contributions that come from a wide range of viewpoints, experiences, and knowledge.

DOCUMENT CONTROL

Document Location:	**Kagumo Teachers' Training College**
Sign off	
Reviewers	**Role**
Mrs. Irene Mwangi	Chief Principal, Secretary to the Board of Management
Pro. Beatrice N. Warue	Board of Management Chairperson

DOCUMENT AMENDMENT RECORD

Issue	**Amendment Detail**	**Author**	**Date**
Edition 1 Revision 0	Development	ICT Officer/ ICT Governance Committee	6th December 2024
	Approval	Board	21st March 2025
Edition 1 Revision 1	Development	ICT Officer/ ICT Governance Committee	
	Approval	Board	

POLICY APPROVAL

The ICT policy has been approved and issued under the signature of:

Mrs. Irene Mwangi **Signed**  **This Date 17/7/2026**
CHIEF PRINCIPAL

Mr. Joanally Ndegwa Kiririu **Signed**  **This date 7/7/2026**
CHAIRPERSON, BOARD OF MANAGEMENT

FOREWORD

Kagumo Teacher's Training College has actively participated in the implementation of the wider government of Kenya policies and the Vision 2030 Strategy among others. In this regard, the college has set up internal structures to manage the reform initiatives necessary to enhance efficiency and effectiveness in teacher training management program. This has been done in keeping with its vision statement ***"A Transformative, Self-directing and Competent Teacher"***. We have since integrated the following systems: ERP for the college operations, e-assessment system provided by Kenya National Examinations Council (KNEC) and in the near future e-learning system.

However, the college acknowledges the fact that it has not been able to keep pace with technological advancement in service delivery. The field of ICT has become more complex and dynamic, both in terms of technologies available and skills required. The college has all a long operated without an explicit I.C.T policy to guide its capacity utilization and address the emerging issues in this field. The Challenges for the college are therefore to develop a *clear vision* and the appropriate *implementation plan* that will anticipate technological changes and identify ***ICT opportunities*** **outside the** ***traditional work practices***. The development of this policy has therefore become a priority if the college is to realize the benefits that I.C.T promises.

Information and communication technologies (ICTs) which include radios and television, as well as newer digital technologies such as computers and the internet are potentially powerful enabling tools for educational change and reform. When used appropriately they will help expand access to education, strengthening the relevance of education to increasingly digital work place and ***raise educational quality by, among others, helping make teaching and learning into an engaging, active process connected to real life.***

However, the experience of introduction different ICTs in the classroom and other educational settings all over the world over the past several decades suggest that the full realization of the potential educational benefits of ICTs is not automatic. The effective integration of ICTs into education system is a complex, multifaceted process that involve not just technology- indeed given enough initial capital, getting the technology is the easiest part.

But also, curriculum and pedagogy, institutional readiness, teacher competencies and long-term financing, among other are a must.

This policy has *"arrived"* at the right time at Kagumo Teachers' Training College intending to *streamline the use of ICT in educational reforms.* The policy comes in handy defining a legal framework for the appropriate and effective use of ICTs in our educational system. It seeks to address the four broad issues in the use of ICTs in education- effectiveness, cost, equity and sustainability. I urge all stakeholders to join me in taking our institution to greater heights of success through implementation of this and other relevant policies.

Prof. Beatrice N. Warue **Signed This Date_____**

CHAIRPERSON, BOARD OF MANAGEMENT.
KAGUMO TEACHERS' TRAINING COLLEGE

PREFACE

Globalization and technological change - processes that have accelerated in tandem over the past fifteen years - have created a new global *economy "powered by the technology, fueled by information and drive by knowledge"*. The emergence of this global economy has serious implications for the nature and purpose of educational institutions. As the half –life of the information continues to shrink and access to information continues to grow exponentially, schools and training institutions cannot remain mere venues for the transmission of a prescribed set of information from teacher to student over a fixed period of time. Rather, schools must promote "learning to learn" i.e. the acquisition of knowledge and skills that make possible continuous learning over the life time.

One of the many challenges facing developing countries today is preparing their societies and governments for globalization and the information and communication revolution. Policy makers, business executives, academics, and ordinary citizens are increasingly concerned with the need to make their societies competitive in the emergent information economy. According to futurist, Alivin Toffler who postulated that *"the illiterate of the 21st century, will not be those who cannot read and write, but those who cannot learn, unlearn and re-learn".*

Kagumo Teachers' Training College share in the belief that with enabling information and communication technologies, we can face future challenges of the information age. With Information and communication technologies, we can leap forth to higher levels of educational, social-cultural, economic and political development. We hope that in making this leap, students and teachers, policy and decision makers and others will find this policy on the information economy, society, and polity useful.

The policy aims at *streamlining the application of ICT infrastructure in the education sector to suit the 21st century challenges, technologies and trends with regards to educational information age.* It underpins the pedagogies and sophisticated modern tools that learners and teachers can embrace during the teaching and learning sessions. *The bottom-line is streamlining the integration of ICT to meet the unique needs of the college.*

The policy will also help planners and decision makers in addressing pertinent issues and crafting policies and strategies appropriate for the use of digital technologies. ICTs *are*

potentially powerful tools for extending educational opportunities, both formal and non-formal, to previously undeserved constituencies-scattered and rural populations, groups traditionally excluded from education due to cultural and social reasons such as ethnic minorities, girls and women, persons with disabilities, and the elderly, as well as all others who for reasons of cost or because of time, constraints are unable to enroll at the colleges and campus. I call upon everybody to embrace this policy as we pressed ahead to greater heights of success.

Mrs. Irene Mwangi **Signed This Date**_____

CHIEF PRINCIPAL.
KAGUMO TEACHERS' TRAINING COLLEGE

EXECUTIVE SUMMARY

The Kagumo Teachers' Training College ICT Policy outlines a comprehensive framework to guide the institution in leveraging information and communication technology (ICT) to enhance operational efficiency, promote innovation, and support its mission of providing quality teacher education.

Chapter one provides the policy's background, objectives, and scope. It emphasizes the institution's commitment to integrating ICT in teaching, administration, and research. The introduction defines the role of ICT in achieving the college's strategic goals, ensuring a robust digital transformation framework.

Chapter two details guidelines for the development, deployment, and management of information systems. It highlights principles for ensuring system reliability, scalability, and user-friendliness, while focusing on enhancing teaching, learning, and administrative functions. Emphasis is placed on the integration of systems for seamless data sharing and improved decision-making.

Chapter three establishes standards for the procurement of ICT resources, ensuring they align with the college's needs and budget. The policy promotes value for money, vendor-neutrality, and adherence to sustainability principles, while prioritizing innovative technologies that enhance educational delivery and institutional operations.

Chapter four focuses on capacity building for staff and students, highlighting training programs, continuous professional development, and digital literacy initiatives. It aims to empower users to maximize the potential of ICT tools, ensuring they are proficient and adaptable to technological advancements.

Chapter five outlines' measures for safeguarding the college's ICT infrastructure against threats. It addresses access control, risk management, disaster recovery, and cybersecurity awareness. The policy ensures the integrity, availability, and confidentiality of institutional data and systems.

Chapter six establishes protocols for the ethical collection, processing, and storage of personal and institutional data. It ensures compliance with data protection laws and promotes transparency, accountability, and respect for individual privacy rights.

Chapter seven underscores the importance of inclusive technology by ensuring that ICT resources are accessible to all, including persons with disabilities. It advocates for compliance with accessibility standards, equitable resource distribution, and the removal of digital barriers.

Chapter eight provides a framework for assessing the implementation and impact of ICT initiatives. It defines Key Performance Indicators (KPIs), feedback mechanisms, and reporting structures to ensure continuous improvement and alignment with institutional goals. The final chapter offers a roadmap for operationalizing the ICT policy. It outlines the roles and responsibilities of stakeholders, timelines for key activities, resource allocation, and strategies for fostering collaboration and compliance.

TABLE OF CONTENTS

CONTENTS **PAGE**
A BRIEF BACKGROUND OF THE COLLEGE ..... **iii**
OUR VISION, MISSION AND CORE VALUES ..... **iv**
DOCUMENT CONTROL ..... **v**
DOCUMENT AMENDMENT RECORD ..... **v**
FOREWORD ..... **v**
PREFACE ..... **viii**
EXECUTIVE SUMMARY ..... **x**
TABLE OF CONTENTS ..... **xi**
LIST OF TABLES ..... **xv**
LIST OF ABBREVIATIONS AND ACRONYMS ..... **xvi**
DEFINITION OF TERMS ..... **xvii**
CHAPTER ONE **1**
INTRODUCTION **1**
1.1 Introduction 1
1.2 Background 1
1.3 Purpose 2
1.3.1 Modernizing Education Delivery 2
1.3.2 Enhancing Administrative Efficiency 2
1.3.3 Building Digital Competence 2
1.3.4 Ensuring Data Security and Privacy 2
1.3.5 Promoting Equity and Accessibility 2
1.3.6 Aligning with National and Global Standards 3
1.3.7 Fostering Innovation and Research 3
1.3.8 Supporting Sustainability 3
1.3.9 Facilitating Continuous Monitoring and Improvement 3
1.4 Policy Statements 3
1.5 Authority 3
1.6 Goals of ICT Policy 4
1.7 Objectives of the ICT Policy 4
1.8 The Scope 4
1.9 Roles and Responsibilities 4
1.9.1 Board of Management 4
1.9.2 Chief Principal 5
1.9.2 Chief Principal 5
1.9.2 ICT Officer 6
CHAPTER TWO **8**
INFORMATION SYSTEMS POLICY **8**
2.1 Introduction 8
2.2 Information Systems 8

2.3 Application Systems 8
2.3.1 Initiation of a Software Project 8
2.3.2 Acquisition 8
2.3.3 Development 9
2.3.4 Maintenance 9
2.4 Operating Systems 9
2.5 Anti-Virus Software 10
2.6 Data Management 10
2.7 Internet-Based Systems 10
CHAPTER THREE 11
ACQUISITION OF INFORMATION TECHNOLOGIES POLICY 11
3.1 Introduction 11
3.1.1 Desktop Computers 11
3.1.2 Laptops 11
3.1.3 Servers 11
3.2 Procurement of Hardware, Software and Other Peripherals 12
3.3 Inventory 12
3.4 Installation 12
3.5 Operation 13
3.6 Maintenance of ICT Equipment Hardware's 13
3.7 Disposal 13
CHAPTER FOUR 14
ICT HUMAN RESOURCE DEVELOPMENT POLICY 14
4.1 Introduction 14
4.2 Objectives 14
4.3 Capacity Building 14
CHAPTER FIVE 15
SYSTEM CONTROLS AND SECURITY POLICY 15
5.1 Introduction 15
5.2 Objectives 15
5.3 Systems Security Control Policy 15
5.3.1 Access 15
5.3.2 Breaches 15
5.3.3 Review 16
5.4 General Physical and Logical Security 16
5.5 Rules, Regulations and Procedures 16
5.5.1 Security of Computers, Software's and ICT Resources 16
5.5.2 Safety of Users and Best Practices 16
5.6 Passwords 17
5.7 Data Security 17

5.8 Copyright and License Agreements 17
5.9 The Internet 17
5.10 Email, Facebook, Chatrooms, Twitters and Video Conferencing 18
CHAPTER SIX 19
DATA PROTECTION POLICY 19
6.1 Introduction 19
6.2 Legal and Regulatory Compliance 19
6.3 Principles of Data Protection 19
6.4. Student Data and Public Usage Policy 20
6.4.1 Consent for Photo and Video Posting 20
6.4.2 Website and Public Display of Student Data 20
6.4.3 Use of CCTV Footage and Surveillance 20
6.4.5. Responsibilities and Accountability 20
6.5 Data Breach Response and Penalties 21
6.5.1 Data Breach Handling 21
6.5.2 Legal Liability and Penalties 21
6.6 Review and Updates 21
CHAPTER SEVEN 22
ACCESSIBILITY IN ICT POLICY 22
7.1 Introduction 22
7.2 Scope 22
7.3 Objectives 22
7.4 Policy Guidelines 22
7.5 Responsibilities 23
7.6 Compliance 24
CHAPTER EIGHT 25
MONITORING AND EVALUATION 25
8.1 Introduction 25
8.2 Monitoring and Evaluation 25
8.3 Compliance 25
8.4 Policy Review 25
Table 8.1 Implementation Monitoring and Evaluation Matrix 27
CHAPTER NINE 29
POLICY IMPLEMENTATION GUIDELINES 29
9.1 Guidelines for Information Systems 29
9.1.1 Application Systems 29
9.1.2 Installation/Operation 29
9.2 Guidelines on Operating Systems 29
9.3 Guidelines on Antivirus Software 29
9.4 Guidelines for Personal Computers and Servers 30

9.5 Guidelines for Procurement 30
9.6 Guidelines on Operations 30
9.7 Guidelines on Inventory of ICT Equipment 30
9.9 Human Resources and Development Guidelines 31
9.9.3 End User Training 31
9.9.4 Technical Training 31
9.9.5 Management Training 31
9.10 System Controls and Security Guidelines 31
9.11 Responsibilities 32
9.11 Systems Access 32
9.12 Physical Security 33
9.12.1 Physical Security Rules 33
9.12.2 Responsibility of The ICT Officer 34
9.12.3 Responsibility of Users 34
9.13 Passwords 34
9.14 Data Security 35
9.14.1 Responsibilities of Users 35
9.14.2 Responsibilities of the ICT Officer 35
9.14.3 Responsibilities of Users 35
9.15 Computer Viruses 36
9.15.1 Responsibilities of The ICT Officer 36
9.15.2 Responsibilities of Users 36
9.16 Accessing Internet 37
9.20.2 Communication 38
ANNEX I: APPROVAL OF THE ICT POLICY AND EFFECTIVE DATE 39
ANNEX II: REPAIR AND MAINTENANCE OF ICT EQUIPMENT PROCEDURE 40
ANNEX III: DATA BACKUP PROCEDURE 43
ANNEX IV: INTERNET CONNECTIVITY AND WEB MAINTENANCE PROCEDURE 45
ANNEX V: KAGUMO TEACHERS' TRAINING COLLEGE ORGANIZATIONAL STRUCTURE 47
ANNEX VI: ICT TECHNICAL COMMITEEE STRUCTURE 48
ANNEX VII: LAN 49
ANNEX VIII: IMPLEMENTATION SCHEDULES 50

LIST OF TABLES

TABLE **PAGE**

Table 8.1 Implementation Monitoring and Evaluation Matrix……....27

LIST OF ABBREVIATIONS AND ACRONYMS

CCTV	Close Circuit Television
CMIS	College Management Information System
DOS	Dean of Students
HOD&S	Head of Department and Sections
HR	Human Resource
ICT	Information Communication & Technology
IIMS	Integrated Information Management System
KNEC	Kenya National Examination Council
MDAs	Ministry, Development, Agencies.
PC	Personal Computer
RPO	Recovery Point Objectives
RTO	Recovery Time Objective
TTC	Teachers' Training College
UPS	Uninterruptible Power Supply unit
WCAG	Web Content Accessibility Guidelines
WWW	World Wide Web
LMS	Learning Management Systems
ISP	Internet service Provider

DEFINITION OF TERMS

Access: Authorized entry to facilities and systems

College: In this policy document refers to Kagumo Teachers' Training College.

Communication Protocols: This means an established procedure for communication that is agreed in advance between two or more parties internal or external to an institution. Such procedure also includes the nature of the information that should be shared with internal and external parties and how certain types of information should be shared with internal and external parties.

Crisis: It is an event, occurrence and/or perception that threaten the operations, staff, shareholder value, stakeholders, brand, reputation, trust and/or strategic/business goals of an institution.

Critical Services: It means any activity, function, process or service, the loss of which would be material to the continued operation of a financial institution.

Disaster: This is a sudden, unplanned catastrophic event that compromises an organization's ability to provide critical functions, processes, or services for some unacceptable period of time causing unacceptable damage or loss.

Emergency Response Team: It's any organization that is responsible for responding to hazards to the general population (e.g. fire brigades, police services, hospitals)

Firewall: Network security system either hardware or software-based that uses rules to control incoming and outgoing network traffic

ICT (Information and Communication Technologies): ICT means technologies, including computers, the internet, WWW, intranet, LAN, telecommunication and audiovisual systems that enable the collection, processing, transportation and delivery of information and communications services to users.

ICT System: An ICT system definition includes, but is not limited to, hardware, software and communications equipment that the college uses to communicate, process and store information. The organization and structures involved in relating all these systems, the information they store and the people involved in the administration and maintenance.

ICT Technical Expert(s)/Team: herein refers to ICT lecturers and other personnel trained and certified in the field of Computer Science.

Local Area Network: is interconnection of more than one computer in different locations for the purpose of sharing resources, storage space and communication.

Logical controls: are measures implemented within computer systems and software to protect data, applications, and IT infrastructure from unauthorized access, breaches, or other cyber threats.

Malware: Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system

Manager/ Supervisor: Person overseeing overall ICT resources in managing access rights and work allocation.

Open-source Software: refers to software with source code that is made available to the public, allowing anyone to view, modify, and distribute it.

Operational Risk: It means the risk of loss from inadequate or failed internal processes, people and systems or from external events.

Peripheral devices: refers to computer and related components such as input/output devices, storage units (memories), scanning devices, cameras etc.

Physical controls: refers to the tangible measures and safeguards designed to protect computer systems, network infrastructure, and data storage facilities from physical threats such as unauthorized access, theft, vandalism, natural disasters, and environmental hazards.

Portal: is an organization's data/information resource accessed via internet for public usage.

Recovery Objective: This means a predefined goal for recovering specific business operations and supporting systems to a specified level of service (recovery level) within a defined period following a disruption (recovery time).

Recovery Point Objective (RPO): Recovery Point Objective describes a point in time to which data, must be restored from backup storage for normal operations to resume if a computer system or network goes down as a result of a disruption.

Recovery Time Objective (RTO): Means the duration of time required to resume a specified business operation. It has two components, *the duration of time* from activation of the business continuity plan and the *recovery of business operations*.

Recovery: This is the rebuilding of a specific business operation following a disruption to a level sufficient to meet outstanding business obligations.

Resilience: Means the ability of an organization, network, activity, process or financial system to absorb the impact of a major operational disruption and continues to maintain critical operations or services.

Risk Assessment: It means the probability and impact of specific threats being realized.

Server: means a "super" computer that is used to store centralized database of the information management system that serves all the workstations.

Single Point of Failure: It is a unique source of a service, activity, and/or process where, there is no alternative and whose loss could lead to the failure of a critical function.

User: Any person who is recognized by the College as having a valid reason to access the College ICT systems whether that access is from within the College or outside the College or any person authorized by way of access rights to use an ICT resource.

Workstation: is a stand-alone computer connected to the local area network. The computer(s) can access the same information from the centralized database based on the privileges given.

CHAPTER ONE

INTRODUCTION

1.1 Introduction

The *sessional paper no. 1 of 2005* emphasizes that ICT skills play a key role in promoting educational and economic development in Kenya.

The government of Kenya recognizes an ICT literate workforce as the foundation on which the country can acquire the status of a knowledge-based economy. The MOEST policy on ICT is to integrate ICT in educational administration, planning and training systems. It's therefore imperative that stakeholders should embrace knowledge, skills and attitudes related to the appropriate use of ICT in the college add value to the quality and the growth of the college and country at large.

This policy framework seeks to guide, provide regulatory measure and streamline the usage, provision, acquisition, procurement, maintenance and storage of ICT tools and resources at all times at Kagumo TTC. It also addresses procedures, processes, installation processes, retrieval of data and equipment, communication systems, acquisition and maintenance of hardware and software's, data management and training of human resource personnel.

1.2 Background

In 2023, the College adopted a five-year Strategic Plan and service charter that outlined its overall vision, mission as well as other ways to improve delivery of services. One of the areas that the College is giving considerable attention is the formulation and implementation of an ICT policy and strategy. The College is aware that most institutions in both the public and private sectors are re-defining their policies and strategies to embrace ICT. In the public sector for example, the *e-government strategy and the National ICT Policy* were adopted in 2004 and 2006 respectively. The Ministry of Education Strategy for ICT was later launched in 2006.

The overall objective of the above policies being to improve service delivery in keeping with 21st century challenges. The immediate challenge for college is to establish medium and long-term ICT plan and adoption of an enabling policy. There is also need to harmonized and integrate existing systems, present and future initiatives. In this regard efforts to establish appropriate ICT standards, data security systems and procedures as well as related quality

assurance mechanisms are a priority. In addition, the College will need to address organization reengineering, related staffing issues and ICT staff development.

1.3 Purpose

The rationale for the ICT Policy at Kagumo Teachers' Training College is to establish a comprehensive framework for integrating technology into the institution's operations, ensuring it aligns with its mission of excellence in teacher education. This policy addresses the growing need for digital transformation in education and aims to position the College as a leader in technology-driven learning and administration.

1.3.1 Modernizing Education Delivery

The adoption of ICT enhances teaching and learning by introducing innovative approaches, such as e-learning platforms, multimedia tools, and Learning Management Systems (LMS). The ICT Policy ensures that the College provides a dynamic, interactive, and modern educational experience that meets global standards.

1.3.2 Enhancing Administrative Efficiency

ICT systems streamline key administrative processes, including student registration, records management, communication, and resource allocation. The policy ensures that such systems are adopted and optimized, resulting in more efficient, accurate, and timely service delivery.

1.3.3 Building Digital Competence

The policy aims to equip students and staff with essential digital skills to thrive in a technology-driven world. By fostering digital literacy, the College enhances the employability of its graduates and the productivity of its staff.

1.3.4 Ensuring Data Security and Privacy

In light of increasing cyber threats and the need for compliance with data protection laws, the ICT Policy prioritizes robust data security measures. It protects the confidentiality, integrity, and availability of institutional and personal data.

1.3.5 Promoting Equity and Accessibility

The policy seeks to ensure equitable access to ICT resources for all stakeholders, regardless of their socio-economic backgrounds. This commitment to inclusivity supports the College’s mission to provide quality education for all.

1.3.6 Aligning with National and Global Standards

The policy aligns with Kenya's national ICT strategies and international educational standards, enabling the College to stay relevant and competitive in the global education sector.

1.3.7 Fostering Innovation and Research

By creating an enabling environment for technology-driven research and innovation, the ICT Policy encourages creativity among students and staff. This contributes to the advancement of knowledge and the development of innovative teaching practices.

1.3.8 Supporting Sustainability

The policy advocates for environmentally friendly ICT practices, such as energy-efficient systems and proper e-waste management, contributing to the College's commitment to sustainability.

1.3.9 Facilitating Continuous Monitoring and Improvement

The ICT Policy includes mechanisms for regular monitoring and evaluation, ensuring that the implementation remains aligned with the College's goals and adapts to emerging technological trends.

1.4 Policy Statements

Policy Statement 1: Establish a reliable, adaptive and robust ICT backbone infrastructure connected to high quality regional and national ICT infrastructure.

Policy Statement 2: Raise the level of awareness on use, application, and potential of ICT.

Policy Statement 3: Integrate ICT into college systems at all levels to improve access to, and quality of teaching and training.

Policy Statement 4: Deploy ICT to facilitate effective and efficient service delivery and interaction with the public and students.

Policy Statement 5: Deploy ICT to enhance oversight functions of the college.

1.5 Authority

The policy derives its authority from:

1. The Kenyan constitution 2010 and the National ICT Policy 2020;
2. BETA- Bottom-Up Economic Transformation Agenda
3. Vision 2030;

4. The Kagumo TTC Service Charter 2024-2025;
5. Strategic Plan 2023- 2028;

1.6 Goals of ICT Policy

To integrate secure ICT in learning and college management functions.

1.7 Objectives of the ICT Policy

(i) Infrastructure Development: Establish and maintain robust, reliable, and scalable ICT infrastructure to support academic and administrative functions.

(ii) Digital Literacy: Promote ICT proficiency among staff and students to ensure effective utilization of technology in teaching, learning, and research.

(i) Data Security and Privacy: Implement physical and logical controls to safeguard institutional data and ensure compliance with legal and ethical standards.

(iii) ICT Integration in Education: Enhance pedagogical practices by integrating ICT tools and platforms, including Learning Management Systems (LMS).

(iv) Efficiency in Administration: Deploy ICT in administrative processes.

1.8 The Scope

a) The ICT Policy shall apply to all the College staff, students and stakeholders.

1.9 Roles and Responsibilities

1.9.1 Board of Management

(i) Policy Approval and Endorsement: Review, approve, and formally adopt the ICT policy to guide the institution's ICT initiatives.

(ii) Strategic Oversight: Provide strategic direction for ICT adoption and integration within the institution.

(iii) Resource Allocation: Approve budgets and allocate resources for the implementation and maintenance of ICT systems.

(iv) Compliance and Risk Management: Oversee compliance with relevant legal, regulatory, and ethical standards related to ICT use, such as data protection laws and cybersecurity requirements.

(v) Monitoring and Evaluation: Establish mechanisms for regular review and evaluation of the ICT policy’s impact and effectiveness.

(vi) **Advocacy and Stakeholder Engagement:** Engage with external stakeholders, including government agencies, donors, and private sector partners, to support ICT initiatives.

(vii) Capacity Building: Support initiatives aimed at building digital literacy and ICT competencies among staff and students.

(viii) Sustainability and Innovation: Promote the adoption of sustainable ICT practices, such as energy-efficient systems and proper e-waste management.

(ix) Conflict Resolution and Accountability: Address disputes or issues arising from the implementation of the ICT policy.

1.9.2 Chief Principal

(i) Policy Implementation Oversight: Lead the implementation of the ICT policy and ensure its alignment with the College's vision and mission.

(ii) Leadership and Strategy: Provide strategic leadership in integrating ICT into teaching, learning, and administration.

(iii) Resource Mobilization and Allocation: Mobilize resources for ICT infrastructure, training, and other related needs.

(iv) Capacity Building: Oversee the development and delivery of ICT training programs for staff and students.

(v) Monitoring and Evaluation: Ensure regular monitoring and evaluation of ICT policy implementation, using key performance indicators (KPIs).

(vi) Compliance and Risk Management: Ensure the College adheres to data protection laws, cybersecurity standards, and other ICT-related regulations.

(vii) Stakeholder Engagement: Act as the primary liaison between the Board of Management, ICT Technical Committee, staff, and students on ICT matters.

(viii) **Reporting and Accountability:** Prepare and present progress reports to the Board of Management on ICT policy implementation.

1.9.2 Chief Principal

(i) Implementation of ICT Policy: Develop detailed implementation plans based on the ICT policy.

(ii) **Technical Oversight:** Provide technical expertise in the selection, procurement, and deployment of ICT systems, hardware, and software.

(iii) **System Maintenance and Support:** Monitor the performance of ICT systems and address technical issues promptly.

(iv) **Cybersecurity and Data Protection:** Develop and enforce measures to secure ICT systems and institutional data against cyber threats.

(v) **Training and Capacity Building:** Organize ICT training sessions for staff and students to enhance digital literacy and system usage.

(vi) **Monitoring and Evaluation:** Develop metrics and tools to monitor the performance and impact of ICT initiatives.

(vii) **Advisory Role:** Advise the Chief Principal, Board of Management, and other stakeholders on technical aspects of the ICT policy.

(viii) **Budget and Resource Management:** Assist in preparing budgets for ICT projects, ensuring cost-effective use of resources.

(ix) **Vendor and Partnership Management:** Evaluate and recommend ICT vendors and service providers based on quality, reliability, and cost-effectiveness.

1.9.2 ICT Officer

(i) **Implementation of ICT Policy:** Support the rollout of ICT initiatives and projects outlined in the policy.

(ii) **System Administration and Maintenance:** Manage and maintain the College's ICT infrastructure, including networks, hardware, software, and servers.

(iii) **Technical Support:** Provide technical assistance to staff and students, ensuring smooth use of ICT tools and systems.

(iv) **Cybersecurity and Data Management:** Implement cybersecurity measures to protect the College's data and ICT systems from threats.

(v) **User Training and Capacity Building:** Conduct ICT training for staff and students to improve digital literacy and system proficiency.

(vi) **Monitoring and Reporting:** Monitor the performance of ICT systems and report on their status to the ICT Technical Committee.

(vii) **Procurement and Inventory Management:** Assist in identifying and recommending ICT equipment and software for procurement, maintain an inventory of all ICT resources and ensure proper documentation and ensure that ICT assets are used efficiently and remain in good condition.

(viii) **Innovation and Continuous Improvement:** Research emerging technologies and recommend innovative solutions to enhance teaching, learning, and administration.

(ix) **Collaboration with Stakeholders:** Work closely with the Chief Principal, ICT Technical Committee, and other departments to align ICT services with institutional needs and engage with external service providers to ensure quality delivery of outsourced ICT services.

CHAPTER TWO

INFORMATION SYSTEMS POLICY

2.1 Introduction

The Information Systems (IS) Policy is a crucial component of the broader ICT Policy at Kagumo Teachers' Training College. It is designed to establish a comprehensive framework for the management, use, and security of information systems within the institution.

2.2 Information Systems

a) Information Systems policies are intended to support structured approach to acquisition, development, operations and maintenance of information systems in the College. In this way, the College will guarantee their success and therefore better decision support to meet its mandate.
b) The ICT Officer and its ICT Technical Experts shall be the sole custodian and technical administrator of all Information Systems and Applications in the College;
c) The ICT Officer shall be guided and assisted by its technical experts in order to carry out his/her mandate expeditiously.

2.3 Application Systems

2.3.1 Initiation of a Software Project

a) All software acquired and developed shall be used strictly for Kagumo TTC purposes only.
b) Every software acquisition or development request shall be initiated through a written statement of scope and objective. The written statement will be submitted to the ICT technical committee.

2.3.2 Acquisition

With respect to software acquisition:

a) The College will use packaged software as the preferred option;
b) In the event that custom development of software is proposed, the request for such development must be justified on case-by-case basis;
c) The application software's shall be accompanied by their license / warranty, backups, documentation and technical support;

d) Only open-source software with technical support shall be used with approval by the ICT Technical Committee and the ICT Officer.

2.3.3 Development

With respect to software application development:

a) Each software development project will be initiated on the basis of an approved requirements specification which:
    (i) Identifies user requirements (functional requirements) expressed in non-technical language;
    (ii) Provide return on investment analysis; and
    (iii) Identifies beneficiaries.
b) If the Requirements (specifications) are approved, the project sponsor and owner will proceed with the technical Specification to express user requirements specified in technical language
c) The College shall purchase only fully licensed copies of computer software accompanied by documentation, software license and technical support;
d) User testing and acceptance are the necessary and sufficient conditions for systems commissioning.

2.3.4 Maintenance

Application software maintenance is critical for effectiveness and efficiency of the system. The following policy guidelines will therefore apply:

a) Access to live systems will be restricted to authorized users;
b) Application software purchased must have service level maintenance agreements to ensure continuity;
c) Only certified supplier or authorized agents will be allowed to provide maintenance;
d) Internal maintenance shall be provided by ICT Technical personnel trained and certified; and
e) Maintenance contracts for Information systems in the College shall be managed by the ICT Officer and the ICT Technical Committee.

2.4 Operating Systems

The following policies are intended to facilitate the governance of office automation within the College:

a) Microsoft's Windows Operating Systems will be the preferred Operating System for all computers;

b) The ICT Officer shall ensure the operating system is genuine and has license;
c) The College will standardize its office productivity tools on the Microsoft Office suite;
d) Commonly used functions that require the same templates will be supported through issuance of college-specific templates.

2.5 Anti-Virus Software

With respect to anti-virus software:

a) The ICT Officer shall ensure availability and *continuous update* of anti-virus protection on all computers, laptops and servers;
b) No person shall be allowed to connect private PCs, laptops, modems or any ICT peripheral to College's network or hardware without approval from the ICT Officer; and
c) All removable media in use within the College must be scanned for viruses.

2.6 Data Management

In order to ensure that data and information are available as and when required, the following policies will be adopted:

a) It is the responsibility of Heads of Departments and Sections in close consultation with the ICT Officer to determine and design the data that should be available in the College;
b) The ICT Officer will ensure overall data capture, availability, accuracy, confidentiality and integrity;
c) The ICT Officer will acquire systems and tools to create, process, manage and preserve data;
d) The data shall be classified into Confidential and Public.

2.7 Internet-Based Systems

The ICT Officer will adopt and develop the following internet-based systems as a means of communication and service delivery:

a) E-mail systems;
b) Short Message Services;
c) Local Area Network and Intranet;
d) Collaborative systems; And
e) Web sites;

CHAPTER THREE

ACQUISITION OF INFORMATION TECHNOLOGIES POLICY

3.1 Introduction

The objectives of Information Technology policy must be consistent with public sector standards issued by relevant authority such as the Public Procurement Authority and E-Government Secretariat.

3.1.1 Desktop Computers

a) The ICT Officer shall seek to:
   (i) Standardize hardware equipment to minimize multi-brands;
   (ii) Allocate computers to user departments and Sections appropriately;
   (iii) Provide uninterrupted power supply and protection to all ICT installations in order to protect the systems from power fluctuations, surges and lightning; and
   (iv) Review hardware specifications to be in line with current technological trends.
b) Users are accountable for all ICT equipment allocated to them;
c) Any computer and/ or computer accessories that malfunction must be reported to the ICT Officer.

3.1.2 Laptops

With respect to Laptops:

a. Laptops will be procured for All the Departments and Sections areas and assigned to officers whose nature of work merits their use;
b. Hardware and software specifications shall be continuously reviewed to be in line with current technological trends;
c. Users are accountable to the ICT Officer for all laptops issued to them; and
d. There will be no additional software installation without prior authority from the ICT Officer.

3.1.3 Servers

The following best practices will be adhered to with respect to server deployments within the College:

a) Maximization of the storage system;
b) Ensuring online and offsite backups and real-time replication for critical applications;
c) Disaster prevention arrangements;

d) The acquisition of servers should be standardized to avoid multi brands;
e) All servers other than for backing up and disaster recovery shall be located in a central server room;
f) The ICT Officer will be responsible for the administration of all the servers in the College;
g) Provide uninterrupted power supply and protection for all servers; and
h) Review hardware specifications to be in line with current technological trends.

3.2 Procurement of Hardware, Software and Other Peripherals

The procurement of hardware, software, peripherals and network products shall be guided by procurement laws and regulations and:

a. Must conform to minimum technical specifications and standards established by the ICT Officer;
b. Must be informed by annual procurement plans prepared, determined and approved by the ICT Officer and its Technical experts;
c. Take into account software requirements and anticipate future requirements;
d. The chief principal will approve directly procurement of ICT emergency equipment.
e. Be from manufacturers, authorized dealers and/or certified service centre.
f. Must have warranty.

3.3 Inventory

a) The ICT Officer shall establish and maintain an inventory of all ICT equipment in the college;
b) In the event of movement of officers occasioned by deployment or exit, the head of the affected Department/Section shall reallocate any ICT equipment under their custody and communicate the same to the ICT Officer, for purposes of updating the inventory.
c) Movement of ICT hardware from one office to another is restricted.

3.4 Installation

On installation of information technology products:

a. An Installation sing off must be issued by the ICT Officer who shall be involved in the entire installation process;
b. The ICT officer shall be responsible for all installations; and
c. All installations must be in accordance with the supplier standards, Technical and College requirements;

3.5 Operation

a) All operations must have User and Technical manuals from the supplier;
b) The operating environment must conform to the minimum manufacturers' specifications or international standards; and
c) Emergency procedures must be clearly displayed in the server room, laboratories and data centre.

3.6 Maintenance of ICT Equipment Hardware's

Maintenance of ICT equipment is critical for effectiveness and efficiency of the College operations. The following policy guidelines will therefore apply:

a. ICT hardware purchased must have Service Level Maintenance Agreements on expiry of the warranty;
b. Internal maintenance shall be provided by personnel trained and certified;
c. Maintenance contracts for ICT equipment shall be managed by the ICT Officer.
d. Certified manufacturer and/or authorized agents approved by the ICT Officer and technical Team will be allowed to provide maintenance; and
e. Weekly assessment reports on the status of ICT facilities to be provided in soft and hard copies.

3.7 Disposal

Information technology resources disposal must:

a) Be in accordance with the existing public disposal ACT, rules and regulations;
b) Avoid or minimize degradation to the environment;
c) Seek to re-use some of or all the computer components;
d) Seek authority to donate any retired computer equipment;
e) Remove data and systems on all hardware to be disposed off;
f) Comply with manufacturer, supplier or service provider terms and conditions of disposal; and
g) Be indicated on the letter of disposal.

(Note that currently, the operating Public Procurement policies and procedures guided by the Public Procurement and Disposal Act 2005 is in operation)**.**

CHAPTER FOUR

ICT HUMAN RESOURCE DEVELOPMENT POLICY

4.1 Introduction

The ICT Human Resource Development Policy outlines strategies and initiatives aimed at cultivating a skilled, motivated, and dynamic workforce capable of leveraging ICT to achieve organizational goals and foster innovation.

4.2 Objectives

The human resource aspect of ICT is to ensure that the College has personnel who are able to:

(i) Provide effective and efficient support in the development and maintenance of ICT;

(ii) Use ICT to support efficient and effective service delivery;

(iii)Innovate and apply new technology consistent with ICT trends.

4.3 Capacity Building

With respect to capacity building:

a) The ICT Officer will be responsible for the determination of overall ICT training needs and capacity building for all staff, students, employees and agents;

b) The College will provide staff, students and agents with ICT skills and capabilities necessary for use of ICT resources;

c) A skill development programme consistent with the overall Service Charter, strategic plan and Human Resource Development policy will be developed and implemented.

CHAPTER FIVE

SYSTEM CONTROLS AND SECURITY POLICY

5.1 Introduction

a) The College has invested substantially in ICT resources. These resources are vital in realizing the College's business objectives and are integral to the ability of the College to operate effectively;

b) This policy establishes general guidelines, rules and regulations for the use and protection of the College's information and ICT systems. The implementation of this policy will thus promote the availability, integrity and confidentiality of the College's ICT systems.

5.2 Objectives

The objectives of system controls and security policy are to: -

(i) Create general awareness on appropriate security measures that must be implemented to safeguard the effective operation of the College;

(ii) Communicate the responsibilities for the protection of ICT systems;

(iii) Facilitate the preservation of the integrity and privacy (confidentiality) of the Colleges' information; and

(iv) Protect and promote the College's reputation.

5.3 Systems Security Control Policy

The College's ICT systems, and the service it provides, will be protected by effective control of security risks at all levels of the organization, providing, managing and operating to ensure that the requirements regarding availability, confidentiality and integrity are preserved;

5.3.1 Access

Access to the systems will be restricted to authorized users as determined by the head of a service area.

5.3.2 Breaches

Any breach of this policy shall be dealt with under the College's Disciplinary Policy and Procedures. In addition, the College may advise law enforcement agencies of the breach where it considers that a criminal offence may have been committed.

5.3.3 Review

The ICT Officer, ICT technical committee and the ICT Technical Experts shall review this aspect of the ICT policy as need arises. Any changes shall be communicated to all users of the College's ICT systems.

5.4 General Physical and Logical Security

ICT resources are generally exposed to the risk of unauthorized access, manipulation, disruption and natural disasters. In an effort to protect the ICT equipment and systems and ensure their availability, the ICT Officer will:

a) Institute appropriate control measures to ensure that its ICT resources are safeguarded.
b) Appropriate controls will be established to limit access to ICT infrastructure, computer equipment and data, commensurate with the acceptable level of risk;
c) The access to the College's ICT systems shall be reviewed every six (6) months;
d) The ICT technical committee shall conduct an audit of security levels of the existing information systems and their physical security immediately this policy is adopted.

5.5 Rules, Regulations and Procedures

The following general rules and regulations shall apply with regards to conduct, access, usage and maintenance of ICT facilities.

5.5.1 Security of Computers, Software's and ICT Resources

(i) Gaseous fire extinguishers with carbon dioxide shall be installed;
(ii) All cables shall be properly insulated and laid away from users;
(iii) UPS and stand-by generator shall be provided;
(iv) Standardized strong metallic grills and locks on doors, windows and roof(s) shall be enforced;
(v) Unauthorized person(s) shall not be allowed to access ICT facilities;
(vi) Functional CCTV
(vii) Insurance of the property

5.5.2 Safety of Users and Best Practices

(i) Users shall not be allowed to open up metallic covers of computers and other ICT devices;

(ii) Correct procedures shall be followed while starting and/ or closing ICT devices;

(iii) No food, water, or beverages is to be carried to the rooms that has ICT resources;

(iv) ICT officer shall review and publish rules, safety precaution measures from time to time in order to avoid accidental injury to the users and damage to computers.

5.6 Passwords

The ICT department shall prevent unauthorized access to the College's corporate computer systems. Such controls shall take the form of passwords in the user identification process.

5.7 Data Security

The ICT Officer shall develop rules, regulations and guidelines that ensure confidentiality, integrity, access, usage, availability and safety of all College information systems.

5.8 Copyright and License Agreements

a) Only licensed software shall be used in the College. Copying and distribution should not be done without the necessary licenses;

b) The ICT Officer department will ensure that all software applications used by the College complies with the relevant licensing agreements, compile all relevant licensing agreements and maintain a record.

5.9 The Internet

a) To ensure productive, appropriate use and to minimize risks, access to the Internet should be limited to staff and students who need it for their work.

b) Users should use the Internet in an effective, ethical and in a lawful manner.

c) Users should not use the Internet access to view, print, distribute, display, send or receive images, text or graphics of offensive or obscene material or material that violates any Kenyan law.

d) The ICT Officer shall maintain a log of sites visited as a means of determining appropriate usage.

e) The ICT Officer shall install and maintain firewalls to filter content coming in or going out via the internet and protecting external attacks.

5.10 Email, Facebook, Chatrooms, Twitters and Video Conferencing

a) The College encourages the use of email, face book, twitters and other aspects of social media interactions and respects the privacy of users. The College will not routinely inspect, monitor or disclose the contents of email without the consent of the user.

b) However, subject to the requirements for authorization, notification, and other conditions specified in this Policy, the College may inspect, monitor, or disclose email when the College believes that it has a need to do so. The use of email must be related to the College's business activities.

c) Use of email is permitted as long as it does not:

    (i) Violate this policy;

    (ii) Degrade the performance of the network and;

    (iii)Divert attention from work.

CHAPTER SIX

DATA PROTECTION POLICY

6.1 Introduction

Kagumo Teachers' Training College recognizes the importance of protecting personal data and ensuring compliance with relevant data protection laws and regulations. This chapter outlines the measures adopted to safeguard the privacy and confidentiality of student data, particularly when used in public domains such as the institution's website, publications, and social media platforms.

6.2 Legal and Regulatory Compliance

The College shall adhere to the following legal frameworks:

- **The Data Protection Act, 2019 (Kenya)**
- **The Constitution of Kenya, 2010 (Article 31 – Right to Privacy)**
- **General Data Protection Regulation (GDPR) Principles** (where applicable)
- Any other relevant local and international data privacy laws.

6.3 Principles of Data Protection

To ensure compliance with data protection laws, the College will uphold the following principles:

1. **Lawfulness, Fairness, and Transparency:** Personal data shall be processed lawfully, fairly, and in a transparent manner.
2. **Purpose Limitation:** Data shall only be collected for specified, explicit, and legitimate purposes.
3. **Data Minimization:** Only the necessary data required for a specific purpose shall be collected and processed.
4. **Accuracy:** Personal data must be accurate and up to date.
5. **Storage Limitation:** Data shall be retained only for as long as necessary for its intended purpose.
6. **Confidentiality and Security:** Adequate security measures shall be implemented to prevent unauthorized access, loss, or destruction of personal data.

6.4. Student Data and Public Usage Policy

6.4.1 Consent for Photo and Video Posting

- Prior to posting any student photos or videos on the College website or social media platforms, **written consent** must be obtained from the student (if 18 years and above) or from their parent/guardian (if below 18 years).
- Consent forms shall specify how the images will be used and provide an option for students to opt out.
- A **Photo & Media Release Policy** shall be included in the admission forms, allowing students to grant or deny consent at the time of registration.

6.4.2 Website and Public Display of Student Data

- Student personal data (e.g., academic records, contact information, identification numbers) shall **never** be posted publicly without explicit consent.
- Any data published on the website must be anonymized unless permission is granted by the student or legally required.
- Class lists, results, or any academic-related information shall be displayed in restricted-access portals requiring login authentication.

6.4.3 Use of CCTV Footage and Surveillance

- Surveillance footage shall only be accessed by authorized personnel and shall not be shared publicly unless required by law enforcement or with the consent of affected individuals.
- The College shall post visible notices informing individuals of CCTV usage on campus.

6.4.5. Responsibilities and Accountability

- **ICT Department:** Ensures secure data storage, access control, and compliance with this policy.
- **Human Resource & Administration:** Maintains consent records and enforces compliance for staff and student data usage.
- **All Staff and Students:** Must adhere to the data protection policy and report any breaches or misuse of personal data.

6.5 Data Breach Response and Penalties

6.5.1 Data Breach Handling

- Any data breach must be reported immediately to the ICT Department and College Administration.
- Affected individuals shall be notified within 72 hours if their personal data is compromised.
- Steps will be taken to mitigate harm, including legal action if necessary.

6.5.2 Legal Liability and Penalties

- The College shall ensure compliance to avoid lawsuits arising from unauthorized data usage.
- Any staff member or student found misusing personal data shall face disciplinary action, including suspension or dismissal.
- External parties found violating data protection policies will face legal action.

6.6 Review and Updates

This Data Protection Policy shall be reviewed **annually** to ensure alignment with emerging legal and technological changes.

CHAPTER SEVEN

ACCESSIBILITY IN ICT POLICY

7.1 Introduction

The organization is committed to ensuring that all ICT systems, tools, and services are accessible to users of all abilities, including individuals with disabilities. This policy aims to provide equal access to information, communication, and technology resources while promoting inclusivity and compliance with relevant accessibility standards and regulations.

7.2 Scope

This section applies to all ICT systems, tools, websites, applications, hardware, and digital content owned, operated, or used by the organization.

7.3 Objectives

(i) To ensure ICT resources are inclusive and usable by individuals with varying abilities.

(ii) To comply with local and international accessibility laws and standards, such as the Persons with Disability act 2003 and Web Content Accessibility Guidelines (WCAG), or equivalent regional regulations.

(iii) To provide assistive technologies and accommodations as required for users with disabilities.

7.4 Policy Guidelines

1. Design and Development:

    a) All ICT systems and tools must be designed and developed following accessibility standards such as WCAG 2.1 (or the latest version).

    b) Developers and vendors must incorporate features that ensure usability for individuals with disabilities.

2. Procurement of ICT Tools and Systems:

    a) Accessibility must be a key criterion in the procurement and evaluation of new ICT tools, software, and hardware.

    b) Vendors must provide documentation of accessibility compliance for their products.

3. Assistive Technologies:
    a) The organization will provide assistive technologies, such as screen readers, speech recognition software, and alternative input devices, for employees, students, and other stakeholders as needed.
    b) ICT systems must be compatible with commonly used assistive technologies.
4. Training and Awareness:
    a) Regular training will be provided to ICT staff, developers, and content creators on accessibility standards and inclusive design principles.
    b) Awareness programs will be conducted to sensitize employees about the importance of accessibility.
5. Testing and Audits:
    a) Periodic accessibility testing will be conducted on ICT systems and digital content to ensure compliance with accessibility standards.
    b) Users with disabilities will be involved in usability testing to identify and address barriers.
6. Support and Feedback:
    a) An accessibility support service will be available to assist users in accessing ICT systems and resolving accessibility issues.
    b) Feedback mechanisms will be established to allow users to report accessibility challenges and suggest improvements.
7. Policy Updates:
    a) This accessibility policy will be reviewed and updated periodically to align with new accessibility standards and organizational requirements.

7.5 Responsibilities

1. ICT technical committee: Oversees the implementation and monitoring of the accessibility policy.
2. ICT Department: Ensures all ICT systems comply with accessibility guidelines and standards.

3. All Staff and Stakeholders: Contribute to maintaining an inclusive environment by following the guidelines set out in this policy.

7.6 Compliance

Failure to adhere to the accessibility policy may result in corrective actions, including training, system updates, or other measures to ensure compliance.

CHAPTER EIGHT

MONITORING AND EVALUATION

8.1 Introduction

Monitoring and Evaluation (M&E) is a systematic process designed to assess the implementation and impact of the ICT Policy at Kagumo Teachers' Training College. It plays a critical role in ensuring that the objectives of the policy are achieved effectively and efficiently while providing insights for continuous improvement.

8.2 Monitoring and Evaluation

All ICT systems, as with all other assets, are the property of the College. The College therefore reserves the right to monitor these systems to ensure compliance with this policy. The monitoring of the ICT system activities will be carried out in a manner that respects the rights and legitimate interests of those concerned.

a) Users of the ICT systems should be aware that their activities can be monitored and they should not have any expectation of privacy.
b) In order to maintain their privacy, users of the ICT resources should avoid storing information on these systems that they consider private. By using the College's ICT systems, users expressly consent to the monitoring of all their activities within the College's ICT systems.
c) During the implementation of this policy, the ICT Officer will ensure that there is continuous monitoring and evaluation for efficiency, accountability and transparency. The Monitoring and Evaluation will be carried out by the ICT technical committee.

8.3 Compliance

a) All users of the College's ICT systems are required to read the ICT security policy and give a written declaration that they will adhere to the guidelines set out in the document. The signed declaration should be returned to the ICT Officer. A sample declaration is provided in annex i.
b) The college institutional structures shall comply 100% with the implementation of this policy.

8.4 Policy Review

a) This policy will be regularly (annually) reviewed and amended as required to ensure it remains relevant and effective in meeting the Policy objectives and to keep the document updated with technological trends.

b) The responsibility for the ongoing review resides with the ICT Officer and the ICT Technical Experts in conjunction with the ICT technical committee.

c) Any proposals during intervening period should be submitted to the ICT Officer.

d) Any changes to this policy shall be communicated to all users of the ICT systems.

Table 8.1 Implementation Monitoring and Evaluation Matrix

An ICT policy implementation monitoring and evaluation (M&E) matrix provides a structured way to track the progress and evaluate the effectiveness of an ICT policy.

Objective	Indicators	Means of Verification	Frequency of Monitoring	Responsible Party
Infrastructure Development				
Establish and maintain robust, reliable, and scalable ICT infrastructure to support academic and administrative functions.	- Number of new ICT installations completed. - Percentage uptime of ICT systems. - Satisfaction rate from users on infrastructure reliability.	- Procurement records. - Maintenance logs. - User satisfaction surveys.	Quarterly	ICT Officer, ICT Technical Committee.
Digital Literacy				
Promote ICT proficiency among staff and students to ensure effective utilization of technology in teaching, learning, and research.	- Percentage of staff and students trained on ICT tools. - Number of ICT workshops or training sessions conducted. - Improvement in digital literacy scores (pre- and post-training assessments).	- Training attendance sheets. - pre-and post-assessment reports. - Feedback forms.	Semi-Annually	ICT Officer, Training Coordinator.
Data Security and Privacy				
Implement stringent measures to safeguard institutional data and ensure compliance with legal and ethical	- Number of security breaches detected and resolved.	- Security audit reports. - Compliance certifications.	Monthly	ICT Officer, ICT Technical

standards.	- Compliance with data protection laws. - Frequency of system backups.	- Backup logs.		Committee.
ICT Integration in Education				
Enhance pedagogical practices by integrating ICT tools and platforms, including Learning Management Systems (LMS).	- Number of courses hosted on LMS. - Percentage of staff using ICT in teaching. - Student engagement levels on digital platforms.	- LMS usage statistics. - Staff and student surveys. - Class observation reports.	Quarterly	Academic Heads, ICT Officer.
Efficiency in Administration				
Utilize ICT to optimize decision-making, resource management, and communication within the College.	- Reduction in processing time for administrative tasks. - Percentage of automated administrative processes. - Feedback on communication efficiency.	- System usage logs. - Employee feedback surveys. - Comparative performance reports (pre- and post-ICT adoption).	Semi-Annually	Administration Office, ICT Officer.

CHAPTER NINE

POLICY IMPLEMENTATION GUIDELINES

PART A

9.1 Guidelines for Information Systems

The implementation work plan is as provided in Annex IV.

9.1.1 Application Systems

a. The selection of a supplier or system developer should be carried out in accordance with the existing rules and regulations on public procurement.
b. The duplication of copyrighted software or documentation is strictly prohibited unless for backup purposes.

9.1.2 Installation/Operation

The installation and operation of systems will involve the following: -

a. Preparation of end users with awareness and training prior to commissioning of equipment and deployment [This is to ensure best results and to avoid unnecessary calls to user support].
b. Maintenance of full documentation with respect to configurations, changes, and other "as installed" parameters [This will facilitate efficiency in management of operations, especially in the event of staff changes].
c. Software will be installed in accordance with license agreements.
d. Software will be installed and rolled out only after issuance of an acceptance testing certificate.
e. Systems shall be commissioned only after being tested and accepted.

PART B

9.2 Guidelines on Operating Systems

a) Software drivers to support efficient use of the Microsoft Office suite will be accessible centrally from a designated server; and
b) Updates of the Office Productivity software will be carried out as and when new versions are released.

9.3 Guidelines on Antivirus Software

a. Any new computer or laptop shall be installed with the most current antivirus software; and

b. Any virus-infected computer must be removed from the system until it is certified *as being virus free.*

9.4 Guidelines for Personal Computers and Servers

a) Users are required to lodge a report of any malfunction of the computer they use on the prescribed problem reporting system or mechanism to the ICT Officer;
b) Laptops should not be carried out of college building (s) except for official work outside the building;
c) All laptops to be carried outside for external use must be logged;
d) Hardware specifications should be reviewed biannually by the ICT Officer;
e) The operating environment for all data centers and server rooms should be consistent with the manufacturers' specifications;
f) Server storage should be structured logically and space allocation quotas enforced;
g) The ICT experts and the ICT Officer shall receive newly acquired ICT facilities, audit the requirements and only accepts the facilities if they meet the specifications.

9.5 Guidelines for Procurement

a) The ICT Officer shall undertake an annual survey to determine needs and impact of ICT resources in the College;
b) Requests by any department and section for the procurement of ICT related goods and services shall be validated by the ICT Officer;
c) Technical evaluation and inspection of ICT equipment shall be done under the supervision of the ICT Officer and ICT experts strictly on the basis of the technical specifications;
d) Deployment of procured ICT equipment shall be done by the ICT Officer, strictly on the basis of identified and validated needs;

9.6 Guidelines on Operations

Guidelines covered under physical Security sub section *5.4* shall apply.

9.7 Guidelines on Inventory of ICT Equipment

a) Inventory must include serial number, date of issue, location/service area, model, type, head of Department, responsible officer and functional condition.
b) Inventory of computers shall be reviewed and updated continuously.
c) The ICT Officer shall conduct an annual inventory check of all ICT equipment.
d) In the event of any movement of ICT equipment from one office to another, the same should be communicated to the ICT Officer for purposes of updating the inventory.

9.9 Human Resources and Development Guidelines

The Administration will upgrade ICT skills and knowledge of its staff, students and the entire community from time to time. This will include: -

9.9.3 End User Training

It is a requirement that all newly recruited employees must possess basic computer skills. End user training programme will include the following content: -

(i) Refresher course on basic computer user skills;
(ii) Overview of ICT policies and guidelines;
(iii) Skills specific to particular applications; and
(iv) Security and best practices.

9.9.4 Technical Training

Technical training programme will include the following content: -

(i) Support related training (depending on area of assignment and deployment);
(ii) Professional Certification (in the area of specialization);
(iii) Overview of ICT policies and guidelines;
(iv) Security and best practices; and
(v) Advanced Data Communication and networks.

9.9.5 Management Training

This level of training programme will include the following content: -

(i) Basic computer user skills;
(ii) Overview of ICT policies and guidelines;
(iii) Skills specific to particular applications
(iv) Security and best practices;
(v) Use of management reporting tools.

9.10 System Controls and Security Guidelines

a) All users of the College's ICT systems are required to read the ICT security policy and give a written declaration that they will adhere to the guidelines set out in this policy.
b) The signed declaration should be returned to the ICT Officer. A sample declaration is provided in the annex I.

9.11 Responsibilities

1. The ICT Officer has overall responsibility for security management policy. The officer shall:
    a) Ensure compliance, establishment and implementation of the ICT security policy;
    b) Provide support and guidance to assist users in understanding their responsibilities with regard to ICT security;
    c) Accord other officers' specific privileges to access specific data and information.
2. HOD and Sections are responsible for ICT security within their departments. They should:
    a) Ensure that all users who report to them are aware of this policy and are in compliance with it;
    b) Maintain appropriate control to ensure adherence to this policy;
    c) Ensure that breaches of security are dealt with in a coordinated and timely manner and reported to the ICT Officer.
3. ICT Lecturers Shall:
    a) Ensure compliance with the College's ICT security policy;
    b) Gauge the effectiveness of the ICT security measures through regular monitoring programs;
    c) Report to the ICT Officer on the irregularities and any breaches of ICT security policy.
4. Systems Database Administrator: system access rights will be granted by the system administrator.
5. User Responsibilities: The users of the College's information systems are accountable and responsible for:
    a) Understanding and adhering to this policy; and
    b) Notifying any breach of ICT security to the ICT Officer or immediate supervisor.

9.11 Systems Access

a) Access to ICT equipment and systems shall be restricted to authorized users through the use of logon identities, passwords, locks and access control devices.
b) The use of system logon identities shall be unique to each authorized user.

c) All logon identities shall be authorized by at least two managers of the respective system.

9.12 Physical Security

The creation of user identities shall be as follows: -

a) Access to secure areas of the College shall be authorized by the ICT Officer;
b) Access to the College's ICT network shall be authorized by the ICT Officer; and
c) Access to the applications shall be authorized by the appropriate HOD.

9.12.1 Physical Security Rules

a) The College premises, and in particular secure areas, must be physically strong and protected against weather elements and hazards including rain, floods, fire, extreme temperatures, tremors, dust and lightning;
b) Entry into secure areas will be restricted to unauthorized users;
c) Visitors to secured areas shall be permitted only under strict supervision of an authorized ICT Supervisors and managers. a log shall be kept for each visit;
d) Secure areas shall be protected against intrusion by use of appropriate surveillance systems or by security personnel;
e) Combustible material shall not be kept near ICT equipment;
f) Air temperature and humidity must be controlled within acceptable limits;
g) All computer devices must be adequately protected against interruptions to electricity supply;
h) Computing equipment must not be removed from the College's premises unless written approval is given by the ICT Officer or any other relevant authority.
i) Equipment leaving the college premises are accompanied by a valid authorization by way of a gate pass;
j) There is consistency between the serial numbers on the equipment and the gate pass;
k) All non-college ICT equipment coming into the college premises must be declared and registered.

9.12.2 Responsibility of The ICT Officer

a) Access to the server rooms is restricted to unauthorized users and that access is by an access control device;
b) Server rooms are fitted with fire detectors and fire extinguishing equipment. The fire suppression equipment should preferably be set to automatically extinguish fire; and
c) Air conditioning systems are functional in accordance with supplier standards.

9.12.3 Responsibility of Users

Users must:

a) Not remove any computer device from the College's premises without written approval by the ICT Officer, Supervisors and managers;
b) Safeguard their workstations against damage e.g. from dust, water etc.

9.13 Passwords

All users with access to the College ICT systems are responsible for taking appropriate steps in selecting and securing their passwords. Users should ensure that their passwords are periodically changed. It is essential that access to ICT systems should be through the use of strong passwords. The following rules govern the use of passwords:

a) All passwords must be changed on at most a quarterly basis;
b) Passwords will consist of a minimum of 6 alphanumeric characters;
c) Passwords will be kept private i.e. not shared, or written down;
d) Logon IDs and passwords should be suspended after a specified period of disuse;
e) Logon IDs and passwords should be suspended after a set number of unsuccessful log on attempts';
f) Passwords should not be repeated or be similar to previous passwords, application systems will be set to remember the last 5 passwords;
g) Passwords should not be the word "password" or a similar word in English or vernacular;
h) Procedures for forgotten passwords should require that the user be personally identified by Support Services.

9.14 Data Security

a) In the event of confidential information being lost, either through loss of a computing device or other breach in security, the ICT Officer should be notified immediately; No attempts should be made to recover data without authority from the ICT Officer.
b) Personal data such as music, video, images, documents should not be saved on the network server.

9.14.1 Responsibilities of Users

Users should:

a) Not use the same password for the College's system accounts as for other non-College access (e.g., personal internet accounts etc.);
b) Where possible, not use the same password for various College system's needs. For example, users should select one password for the ICT Officer and a separate password for other ICT systems;
c) Never share passwords with anyone,
d) Never write passwords down or store them anywhere in the office, or on any computer system (including Palm Pilots or similar devices) without encryption;
e) Change passwords at least once every quarter;
f) Log off their workstation whenever they are away from the workstation for an extended period;

9.14.2 Responsibilities of the ICT Officer

The ICT Officer must ensure that:

a) A backup policy and procedure that covers all College data is developed;
b) Automation work plan is developed;
c) The necessary storage space for users to store important College information is provided; and
d) Backups of College data are stored in an access-controlled area.
e) Database integrity is achieved;
f) Only authorized software is installed on the ICT systems.

9.14.3 Responsibilities of Users

Users must ensure that:

a) All College data and files are saved on a network server for which they have been assigned as opposed to the local hard disc;
b) Portable computer storage devices must be stored securely when they are not being used; and
c) Portable computer storage devices that are to be disposed off must be done so securely;
d) Copyright and license agreements: All software used on the College's ICT system must be licensed;

Users must not:

a) Install any software on their PCs without the knowledge of the ICT Officer;
b) Copy, distribute or remove software without the written authority of the ICT Officer;
c) Download and install any software from the internet without the written authority of ICT Officer;
d) Should not know the administrator's password of their PC.

PART C

9.15 Computer Viruses

The following rules govern the use of the anti-virus application:

a) All virus definitions must be current and should not be more than two weeks old;
b) Any PC on the network should be scanned for viruses automatically as it boots;

9.15.1 Responsibilities of The ICT Officer

a) Ensure that Anti-virus systems are kept current.
b) Daily administration of the anti-virus application is planned and automatic updates to definitions are made.
c) Apply any updates to the services it provides that are required to defend against threats from viruses.

9.15.2 Responsibilities of Users

Users must ensure that:

a) Their workstations are running an anti-virus application;
b) They should not disable or remove anti-virus applications or the automatic update feature;

c) They should treat any unexpected email attachment suspiciously and delete the email if unsure of the origin;
d) They do not write, distribute or introduce any software known or suspected to be infected with a virus to the College's ICT systems; and
e) That the anti-virus software is updated regularly.

9.16 Accessing Internet

(A). The following rules govern the use of the Internet and network:

a) Use of the Internet is permitted as long as it does not violate this policy and does not degrade the performance of the network and divert attention from work.
b) Use the Internet to Solicit, Reveal or publicize college confidential or proprietary information, which includes but is not limited to: financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships;
c) Damage, alter, or degrade equipment providing internet and network connections thus hindering others in their use of the Internet.
d) The ICT Officer will seek to interlink all its offices through LAN and use of remote access technologies, with selective access granted to staff, students, suppliers, customers, or other partners.
e) The College shall maintain a presence on the Internet and promote interactivity with its clients through its corporate portal.

(B). Users shall not:

a) Download or store music, media or any other files where copyright issues may be of concern;
b) Use the College's Internet facility for running private businesses;
c) Upload, download, or transmit:
    (i) Copyrighted materials belonging to third parties
    (ii) Offensive, fraudulent, threatening or harassing materials
d) Propagate computer viruses, run peer-to-peer software, send and/or receive unofficial files or undertake activities that cause network congestion;
e) Gain unauthorized access to any computing, information, or communications devices or resources

(C.) Email must not be used to:

a) Reveal or publicize confidential or proprietary College information;

b) Send or forward emails containing defamatory, ethnic, offensive, racist or obscene remarks.
c) Send copies of documents in violation of copyright laws;
d) Harass, intimidate or interfere with the ability of others to conduct the College's business;
e) Attempt to breach any security measures on the email system;
f) Attempt to intercept any email transmission without proper authority;
g) Propagate viruses or generate high volume of network traffic that degrades the performance of the network.

PART D

9.20.2 Communication

A. The College shall ensure that the response to a disruption is communicated internally and externally to applicable parties. The communication procedures should:
    a) Ensure that there is a clear plan identifying staff, for communicating internally (within the organization) and externally (to the public) stakeholders.
    b) Establish communication protocols clearly outlining the chain of command;
    c) Develop a directory for all recovery team members including the crisis management and emergency management teams, local emergency response organizations and critical service providers;
    d) Ensure that the directory/contact lists are made available to all team members;
    e) Address obstacles that may arise due to failure in primary communications systems (electricity, mobile phone network, road network);
    f) Ensure that the institution has set up alternative modes of communication;
    g) Ensure that copies of business continuity plans are disseminated to the relevant personnel.

ANNEX I: APPROVAL OF THE ICT POLICY AND EFFECTIVE DATE

This ICT policy and procedures manual was approved by the Board of Management of Kagumo Teachers' Training College on ……during the full board meeting through minute number MIN.BOM……

AUTHORIZATION

BOM Chair:	**Principal/Secretary to theBOM:**
Name: ……	Name: …….....
Signature: ……...	Signature: ….....……
Date: ……	Date: ……..

Official stamp

ANNEX II: REPAIR AND MAINTENANCE OF ICT EQUIPMENT PROCEDURE

1.0 GENERAL

1.1 PURPOSE

The purpose of this procedure is to ensure consistency and accuracy in the undertaking of repair and maintenance activities on ICT equipment by the college.

1.2 SCOPE

This procedure applies to all repair and maintenance activities undertaken by the college on its ICT equipment.

1.3 REFERENCES

a. KAG.TTC ICT Policy 2010

b. KAG.TTC Quality Manual KAG.TTC/QM/MR/02

1.4 TERMS DEFINITIONS

a. ICT: Information and Communication Technologies

b. HoD: Head of Department

1.5 PRINCIPAL RESPONSIBILITY

The ICT officer department shall ensure that this procedure is adhered to.

2.0 METHOD

2.1 Routine Maintenance

2.1.1 The ICT offcer shall ensure that all the ICT equipment undergo routine maintenance on an annually basis during the months of April, August or December holidays subject to availability of funds.

2.1.2 This procedure shall begin with the ICT officer ensuring that a maintenance schedule of all the ICT equipment such as computers, laptops, projectors, still cameras, video camera is prepared as per prescribed format. ***(See appendix 1 for a sample maintenance schedule)***

2.1.3 The user shall hand over to the ICT officer who shall then hand over the maintenance schedule to the Procurement Officer for action and procurement of the required services as

per procurement procedure number 1 in the procurement procedures manual KAG.TTC/PM/MR/09

2.1.4 The ICT officer shall ensure that:

a. A List for the various ICT equipment to undergo the regular maintenance are prepared

b. Record details of the machine before the maintenance activity is undertaken

c. Oversee the maintenance exercise

d. Advice the HOD by handing in a status report of the equipment.

2.1.5 The ICT officer fill a maintenance log card at the end of the maintenance activity. ***(See annex 11 for a sample maintenance log card)***

2.2 Repair of ICT equipment

2.2.1 This activity shall begin with the ICT officer identifying the status or upon user request of ICT equipment on regular basis and forward a status report to the user department.

2.2.2 In case a user reports a malfunction of ICT equipment, the ICT officer shall assess the equipment; record details of the repairs required in the ICT repair and maintenance register and advise the user department on the appropriate way forward. ***(See annex II for a page format of the ICT repairs and Maintenance register)***

2.2.3 The ICT officer shall compile a report detailing the equipment and/services required for the repairs and raise a purchase requisition as per procedure number 2 in the procurement procedures manual KAG.TTC/PM/MR/09

2.2.4 Upon receipt of the part(s) the ICT officer shall instruct user department when the repair activities will be undertaken or outsource where applicable.

2.2.5 Upon undertaking the repair works required, ICT officer shall ensure that the user department signs-off the same in the ICT repair and maintenance register and this procedure shall be deemed complete.

Maintenance Schedule

No	Item/equipment	Technical Specification	Date Purchased	Current Location	Date Serviced	Status Before Servicing		Status After Servicing	Service Due Date	Warranty Status	Remarks

Sample Maintenance Log Card

Equipment Name: ……

Model: ……..

S/N:

Technical Specification:

……

Category: ……..

Date of Manufacture: …….

Date of Purchase: ……

Supplier: ……..

Date Due for 1st Service: …….

Service Details

Date	Servicing Technician	Part(s) Serviced/Replaced/Upgraded	Servicing Technician Signature	College Technician Signature

ICT Repairs and Maintenance Register

DATE	Equipment	Department	Faults Identified	Departmental staff	Repairs/Maintenance activity undertaken	Date of the repairs	Dept. Sign	ICT staff sign	Remarks

ANNEX III: DATA BACKUP PROCEDURE

1.0 GENERAL

1.1 PURPOSE

The purpose of this procedure is to ensure effectiveness and consistency in the undertaking of data backup by the college.

1.2 SCOPE

This procedure applies to all activities undertaken in backing up data by the college.

1.3 REFERENCES

a. KAG.TTC ICT Policy 2010

b. KAG.TTC Quality Manual KAG.TTC/QM/MR/02

1.4 TERMS DEFINITIONS

a. ICT: Information and Communication Technologies

b. HoD: Head of Department

c. MIS: Management Information System

1.5 PRINCIPAL RESPONSIBILITY

The ICT officer department shall ensure that this data backup procedure is adhered to.

2.0 METHOD

2.1 In undertaking the data backup, the ICT officer shall ensure that the work from different departments is saved in their respective departmental folder Using cloud back up.

2.2 The ERP Server is set to auto backup after every transaction.

2.3 The ICT officer shall ensure the security of the server rooms are maintained and ensure only authorized members access the same.

2.4 When the server is undergoing routine maintenance, the ICT officer shall ensure that the data is backed up using available storage devices before commencement of the same and this procedure shall be deemed complete.

Data Back Up Register

No	User Name	Department	Document Backed up	Backup Medium	Date Backed up	Receiving Technician	Safe Custodian Signature	Remarks

ANNEX IV: INTERNET CONNECTIVITY AND WEB MAINTENANCE PROCEDURE

1.0 GENERAL

1.1 PURPOSE

The purpose of this procedure is to ensure effectiveness and timeliness in the maintenance of internet connectivity and the college's website.

1.2 SCOPE

This procedure applies to all activities undertaken by the college in the maintenance of internet connectivity and the college's website.

1.3 REFERENCES

c. KAG.TTC ICT Policy 2010

d. KAG.TTC Quality Manual KAG.TTC/QM/MR/02

1.4 TERMS DEFINITIONS

c. ICT: Information and Communication Technologies

1.5 PRINCIPAL RESPONSIBILITY

The ICT officer shall ensure that this procedure is adhered to.

2.0 METHOD

2.1 The ICT officer in liaison with the chief principal shall ensure that an Internet service Provider (ISP) is identified as per procurement procedure number 1 of the procurement procedures manual KAG.TTC/PM/MR/09

2.2 The ISP shall maintain the link up to the IDU (Indoor Unit).

2.3 The ICT officer shall ensure that the Local Area Network is well maintained, report any failing points or devices to the ICT officer soonest possible and record the same in the ICT repair and Maintenance Register.

2.4 Upon receipt of any failure report, the ICT officer shall prepare an internal or purchase requisition for the required items as per purchase requisition and internal requisition

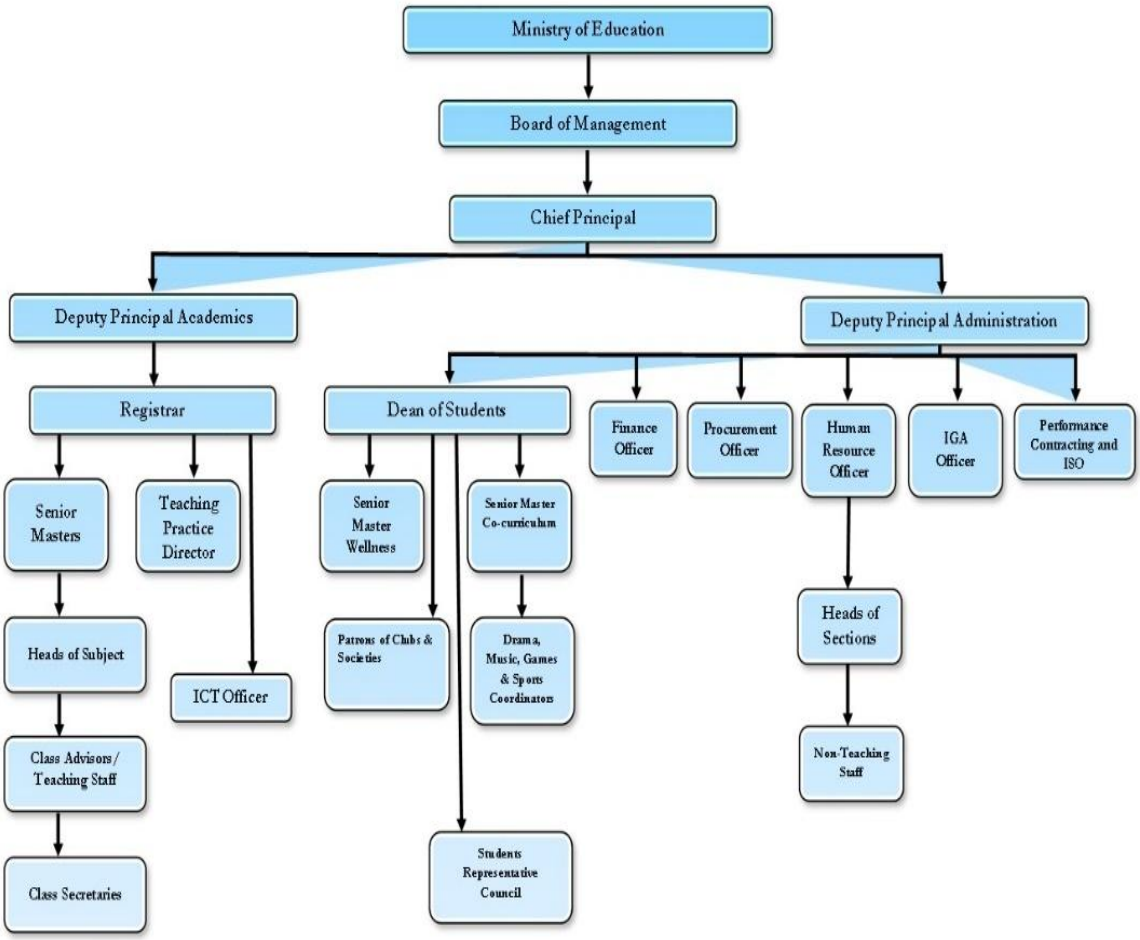
procedures number 2 and 3 respectively in the procurement procedures manual KAG.TTC/PM/MR/09.

2.5 Upon receipt of required items the ICT officer shall ensure that the failures are fixed.

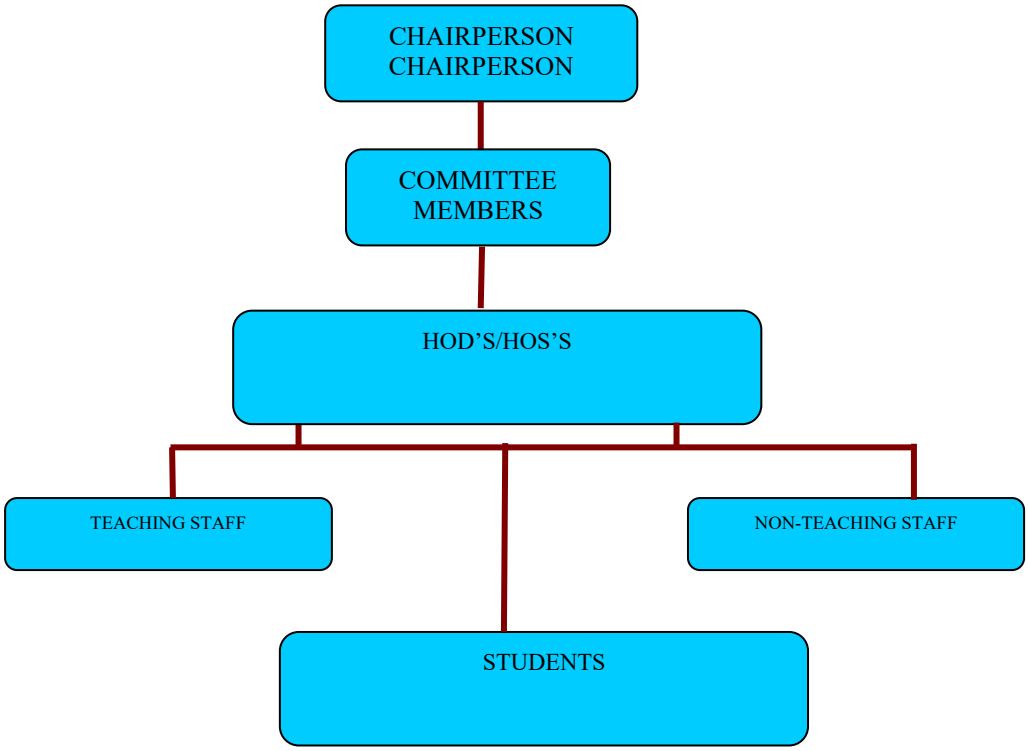
2.6 The ICT officer shall ensure network security and shall issue passwords to the users.

2.7 The ICT officer shall manage the internet bandwidth quotas in line with usage and period of time especially during outage and this procedure shall be deemed complete.

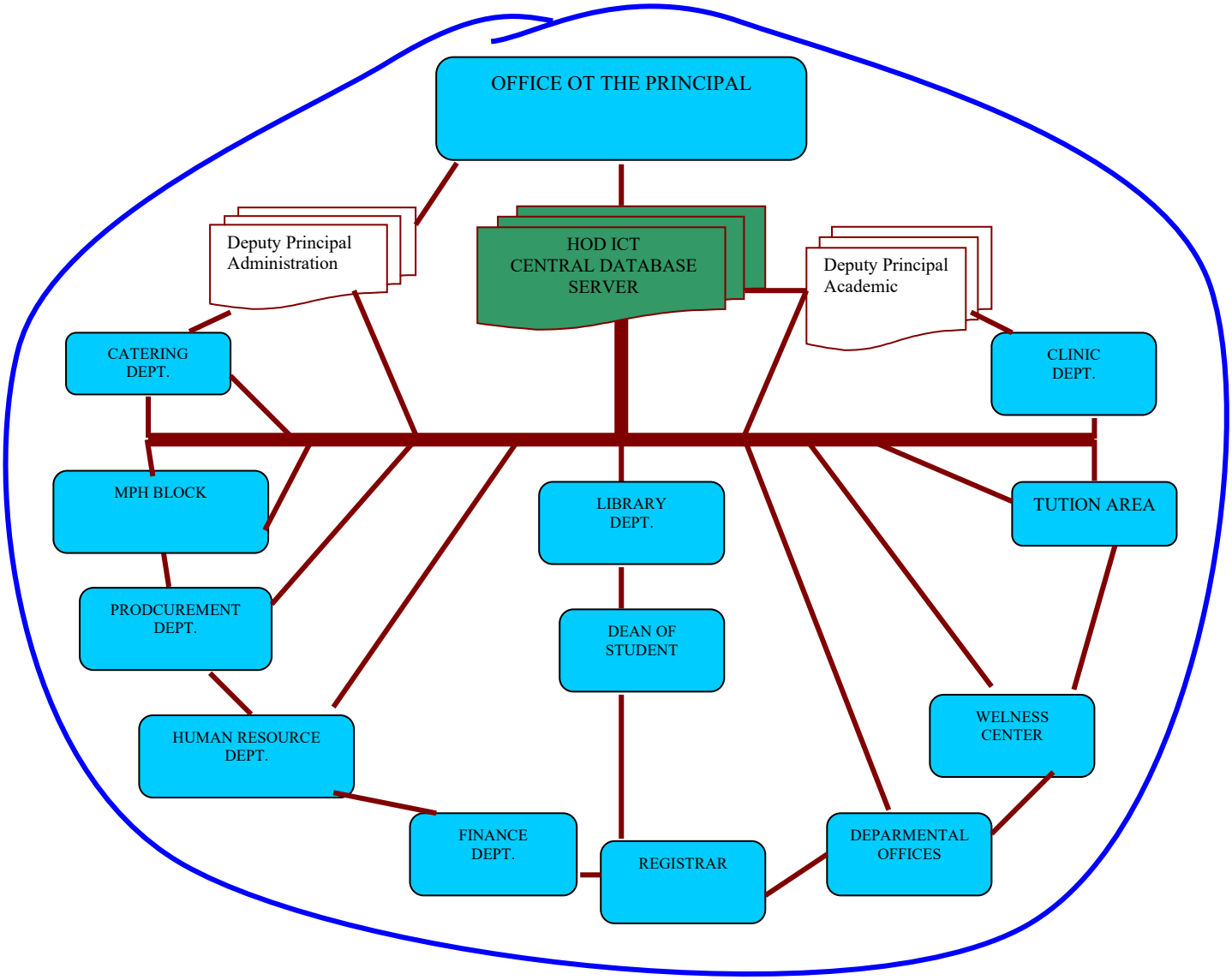
ANNEX V: KAGUMO TEACHERS' TRAINING COLLEGE ORGANIZATIONAL STRUCTURE



ANNEX VI: ICT TECHNICAL COMMITEEE STRUCTURE



ANNEX VII: LAN



ANNEX VIII: IMPLEMENTATION SCHEDULES

	ACTIVITY	*RESPONSIBILITY*	*COST (KShs.)*	**TIMEFRAME**
1	Finalize ICT Draft Policy	ICT Technical Committee	-	3rd Dec. 2024
2	Create awareness of the existence of ICT policy	ICT Officer	-	17th Jan. 2024
3	Board of Management Approval of the ICT Policy	Chairperson, BOM	-	21st March 2025
3	Take inventory of ICT resources	ICT Officer	-	31st Dec. 2024
4	Audit ICT resources	ICT Officer	-	30th March. 2024