KENYA INSTITUTE OF SPECIAL EDUCATION

ICT POLICY

August 2021

Table of Content

Vision

An inclusive Kenyan Society in which every child with special needs and disability accesses quality education and achieves their full potential.

Mission

To facilitate service provision for persons with special needs and disabilities through human capital development, research, data management, functional assessment, rehabilitation, inclusive education practices, technology and production of educational resources and assistive devices.

Core Values

Professionalism,
Relevance,
Integrity,
Equity,
Respect and
Empathy.

Core Functions

The Institute is mandated to carry out the following functions:

1. Conduct teacher training courses for teachers in various fields of education of children with special needs and disabilities
2. Conduct in-service courses for personnel working in all fields of special needs education
3. Prepare and conduct correspondence courses for personnel in the field of special needs education
4. Run an educational and psychological assessment centre for the training of teachers of children with special needs education
5. Run an orientation and mobility centre for training and demonstration purposes
6. Run a model training unit for the integration and inclusion of children with special needs and disabilities into the regular schools
7. Run a pre-school department where training and the stimulation of young children with special needs and disabilities can be carried out for the purpose of teacher training
8. Function as a resource centre for the production and dissemination of information to the general public on special needs and disabilities
9. Run a documentation and resource centre on special needs and disabilities
10. Conduct research in special needs education
11. Maintain, repair, design, produce and assemble special materials and equipment for persons with special needs and disabilities

Foreword

Kenya Institute of Special Education (KISE) is mandated to train personnel in special needs education and offer related services. Use of Information and Communications Technology (ICT) is vital in ensuring achievement of its mission and vision. KISE acknowledges the importance of utilizing ICTs in service provision, research and innovation for its benefit and society. Efficient implementation of ICT requires a guiding framework that will ensure management, compliance, value creation, and support realization of the Institute's objectives.

The adoption and utilization of Information and Communications Technology (ICT) within the Institute is aligned to the Constitution of Kenya 2010, National Information, Communications and Technology (ICT) Policy 2019 and Institute's Strategic Plan 2018-2023.

This Policy provides guidance to all ICT operations and shall assist the Institute in ensuring access to best practices for identification, protection and management of ICT.

Dr. John Mugo
CHAIRPERSON, KISE COUNCIL

Acknowledgement

This Policy is developed in line with the National Information, Communications and Technology (ICT) Policy (2019) to realise the Institute's ICT potential in service provision to staff, students and stakeholders. The Management of Kenya Institute of Special Education wishes to acknowledge with gratitude the incredible contribution of staff who were involved in the development of this "Information Communication and Technology (ICT) Policy". The introduction and operationalization of this policy framework shall ensure efficiency in systems management and service provision in the Institute.

Implementation of ICT policy establishes a framework for governing ICTs and ensures that the Institute adapts to the dynamic technology field. Achievement of the objectives of this policy calls for cooperation from all Institute staff. In addition, it will put the institute in a competitive edge in utilization of technology.

DIRECTOR

Abbreviations

AD/DC	Active Directory/Domain Controller
CCTV	Closed Circuit Television
CD	Compact Disk
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
ERP	Enterprise Resource Planning
ICT	Information Communication and Technology
ICTA	Kenya Information and Communication Technology
LAN	Local Area Network
MFP	Multi-Purpose Printer
NESSP	National Education Sector Strategic Plan
PPADA	Public Procurement and Assets Disposal Act
PWD	Persons with disabilities
SLA	Service Level Agreement
TNA	Training Needs Assessment
UPS	Uninterrupted Power Supply
WAN	Wide Area Network
WCAG	Web Content Accessibility Guidelines

Definitions of Key Terms and Concepts

Adaptations: Redesigning of implements, tools, equipment, machines, workstations, work environment to suit individual needs of persons with disabilities.

Assistive Technologies: Tools provided to persons with disabilities to assist them in employment, training, development and any other activities in learning environment or at the workplace.

Computer virus: a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code. When this replication succeeds, the affected areas are then said to be "infected" with a computer virus. This includes malwares

Cyber-attack: any offensive maneuver that targets computer information systems, infrastructures, computer networks, or personal computer devices.

Cyber threat: any malicious act that attempts to gain access to a computer network without authorization or permission from the owners.

Data corruption: refers to errors in computer data that occur during writing, reading, storage, transmission, or processing, which introduce unintended changes to the original data.

Deployment: All of the activities that make a software system available for use.

Hardware Sanitization: The process of deliberately, permanently and irreversibly removing or destroying the data stored on a memory device to make it unrecoverable.

Malware: any software intentionally designed to cause damage to a computer, server, client, or computer network. A wide variety of malware types exist, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, wiper and scareware.

Persons with disabilities: These are persons who have long-term physical, mental, intellectual or sensory impairments and/or chronic conditions which in interaction with various barriers may hinder their full and effective participation in society on an equal basis with others.

Redundancy: Having extra or duplicate resources available to support the main system. It is a backup or reserve system that can step in if the primary system fails.

Workstations: Workstations constitute critical ICT infrastructure that ensure service provision is carried out in the most effective and efficient way. They include laptops, desktops, tablets and authorized home workstations accessing the Institute's network.

Chapter One: Introduction

The Institute developed its Strategic Plan for 2018-2023 taking cognizance of changes in the operating environment. Information Communication and Technology (ICT) is a key mover and driver in stimulating creativity and innovation.

This policy is intended to provide a framework for acquisition, deployment, usage and exploitation of ICT resources to automate and transform all Institute business processes. In addition, it will guide further development, administration, maintenance and optimum utilization of ICT resources within the Institute.

1.1 Legislative and Policy Framework

The following legal frameworks provide a basis for implementation of this policy:

1. The Constitution of Kenya, 2010
2. Persons with Disability Act, 2003
3. The Basic Education Act, 2013
4. Kenya Information and Communication (Amendment) Act, 2013
5. Media Act, 2013
6. Kenya Information and Communication Technology (ICTA) order, 2013
7. National Education Sector Strategic Plan (NESSP), 2018-2022
8. National Information, communications and Technology (ICT)Policy, 2019
9. Data Protection Act, 2019

1.2 Rationale

It has become critical to enact an ICT policy to ensure an enabling mechanism for efficient service delivery, information sharing, electronic operations and management of ICT resources.

1.3 Scope

This policy applies to all ICT equipment, software, facilities and ICT facilitated processes in the Institute. It shall be a reference document on ICT standards for Institute staff, students and anyone accessing/developing/implementing and/or using ICT-based information and resources owned by the Institute.

1.4 Guiding Principles

This policy shall be guided by the following key principles:

1. Making ICT in the Institute available, accessible and easy to use for all;
2. Seamless integration and ICT support in all Institute operations;
3. Adherence to best practices, policies and ethics;
4. Sustained training and technical support;
5. Continuous systems and business process improvements.

1.5 Objectives

This policy aims to strengthen the use of ICTs in all Institute operations to support its strategic direction by improving operational efficiency and exchange of information so as to maintain a competitive edge. The specific objectives of this policy are to:

1. Provide efficient, accessible and reliable ICT facilities, services and automation.
2. Provide guidance in developing a reliable and secure ICT infrastructure that conforms to recognized standards supporting all services in the Institute.
3. Provide ICT infrastructure and services responsive to the needs of persons with disabilities.
4. Facilitate adaptations to new technologies, tools and models to respond to challenges posed by ICT
5. Promote information sharing, transparency, accountability and reduced bureaucracy in operations
6. Ensure information security of the Institute systems and data
7. Promote efficient utilization of information systems within the Institute

Chapter Two: Policy Focus Areas

Introduction

This chapter covers policy statements and strategies for implementation. These include: security, training and research, acquisition and disposal, backup and disaster recovery, accessibility for PWDs, use of ICT resources, network management, classification of information, third-party services management, security risk assessment and audit, cyber security awareness, skills development, and management and maintenance.

2.1 Security

Policy statement

The Institute shall ensure appropriate security for all data, equipment, and processes in its ownership and control.

Strategies:

a. Protect the Institute’s information and communications systems from unauthorized access, use, disclosure, disruption, modification, or destruction by ensuring that:
   - i. All server rooms are kept secure under biometric access control and only authorized personnel shall be allowed entry.
   - ii. Non-ICT staff working in the server room shall be supervised at all times.
   - iii. Server rooms shall be installed with air conditioning system and uninterrupted power supply (UPS) units in order to provide a stable operating environment.
   - iv. Classified data shall not be transmitted unencrypted across unsecured electronic communication links.
   - v. Only the Institute's standard approved software shall be installed

b. Appropriate measures shall be taken when using workstations to ensure confidentiality, integrity and availability of information.
   - i. Each user shall have a unique username and password with access levels and privileges. Where necessary, biometric data shall be collected to facilitate access and service provision.
   - ii. All devices shall require access credentials (user ID and password) to be accessed over the network.
   - iii. Users shall be responsible for confidentiality of their access credentials and prevention of any unauthorized access to ICT equipment. Any attempt to use other users’ credentials to gain access to network resources is prohibited.
   - iv. The Human Resource and Academic Registrar’s Office shall establish mechanisms whereby changes in employment status shall be communicated immediately to the ICT office.
   - v. Access credentials shall immediately be deactivated and confirmed in a clearance certificate by the ICT Office once a member of staff ceases to be an employee of the Institute.

vi. All computers connected to the Institute network, shall be running an up to date antivirus programme with latest virus signature definitions.

vii. ICT Office is authorised to gain access to a user account and folder of an account suspected to have breached systems security or is in violation of this policy.

viii. The Institute shall follow sound professional practices in providing for security of electronic messaging system.

ix. Users shall not install, email, transmit or otherwise make available any material that contain malware, confidential information or programmes designed to interrupt, destroy or limit functionality of any computer software or hardware.

c. The Institute shall install Closed Circuit Television (CCTV) systems to aid in prevention, investigation and detection of crime. It will also facilitate monitoring of security and safety of premises.

i. Institute security office shall be the custodian of CCTV equipment and responsible for viewing live feed.

ii. Retrieval of video files shall be facilitated by ICT office upon written approval by the Director.

iii. The Institute shall be under CCTV surveillance at all times and visitors shall be made aware.

d. All network or systems software malfunctions, information security alerts, warnings, suspected vulnerabilities, and the like, and suspected network security problems, shall be reported immediately only to the ICT Office. To monitor and respond to security incidences, the ICT Office shall:

i. establish an incident detection and monitoring mechanism to detect, contain and ultimately prevent security incidents.

ii. manage the ICT service desk and incidents, to enable effective use of ICT systems by ensuring resolution and analysis of end user queries, questions and incidents.

iii. make users aware of the security incident handling/reporting procedures in place

2.2 Training and Research

Policy statement

Various infrastructure shall be put in place to support networked learning, other e-learning approaches and research. The Institute shall put in place mechanisms for continual improvement.

Strategies

a. To ensure only authenticated students access online classes, the Institute shall adopt the use of an e-learning management system.

b. The bandwidth management shall give priority to academic content, research, Institute website and official email facility over general Internet browsing and other utilities.

c. All lecture rooms shall be fitted with infrastructure for multi-media teaching and learning to enable implementation of e-learning and other blended learning approaches.

d. The Institute library shall be fitted with ICT infrastructure to support e-resources for enhancing learning and research. Where possible and desirable, open source learning systems shall be used to reduce cost and also allow for customization.
e. The institute shall deploy appropriate technology to carry out research.
f. Student assignments and project work shall be presented in soft copy on CDs. All submitted work shall be tested for plagiarism using authorized software.
g. Where possible, electronic continuous assessment shall be designed and delivered to students. The assessment system shall become a mission critical system that will be secured and provided with redundancy.
h. Trainers and technicians shall provide basic training on ICTs to new students on use of facility(s).

2.3 Acquisition and Disposal

Policy statement

Acquisition of ICT resources shall be based on intended use, conformity to standards and regulations, cost (acquisition, maintenance and disposal) and ease of integration with existing ICT infrastructure.

Strategies

a. ICT office shall coordinate automation of an updated inventory of hardware and software that is in use by the Institute.
b. Equipment that cannot be serviced by ICT office shall be placed on outsourced service contracts
c. Acquisition and Disposal of ICT facilities shall be guided by the Public Procurement and Asset Disposal Act (PPADA), 2015 and be in line with government ICT standards.
d. All user requests for acquisition of ICT equipment and services shall be channeled through the ICT Office. The office shall prepare specifications in consultation with the requesting user.
e. The Institute's surplus and/or obsolete non-leased ICT assets and resources shall be disposed of in accordance with standards and procedures in a cost-effective manner in compliance with legal and environmental requirements.
f. Hardware sanitization shall be undertaken to protect the Institute's intellectual property and the confidentiality of Institute data residing on all hardware.
g. After hardware sanitization, ICT assets and equipment for disposal shall be handed over to the Assets Disposal Committee for further action.
h. All hardware donations to the Institute from any source shall be subject to ICT office check for suitability and fit–for-purpose.
i. ICT office shall scrutinize any hardware and software license agreements with vendors and Service Level Agreements (SLAs) and advise management accordingly.
j. The Institute shall establish and define a lifecycle for all ICT equipment to provide a balance between optimum use and on-going maintenance costs.

2.4 Backup and Disaster Recovery

Policy statement:

The Institute shall maintain consistent data backup and recovery measures to ensure business continuity in the event of data corruption or loss. This shall be in line with the Institute risk management framework.

Strategies

a. The Institute shall establish and maintain a disaster recovery site in line with the disaster recovery plan.
b. Scheduled backup of Institute's centralized systems and servers shall be performed and uploaded to an offsite location for safekeeping.
c. Backed up files shall be subject to verification on a quarterly basis where restoration will be simulated on an identified machine dedicated for this task. Once restored, the system shall undergo testing to ensure successful data reinstatement to its intended state.
d. Removable backup media shall be stored in a locked fireproof safe in a room that is access-controlled
e. The retention period and any requirement for archive copies shall be determined for critical business information as well as based on any legal requirements.

2.5 Accessibility for PWDs

Policy Statement

The Institute shall provide ICT services and infrastructure that is responsive to the needs of Persons with Disabilities (PWDs). This shall be in line with the Institute's Disability Mainstreaming Policy.

Strategies

The Institute shall:

a. customize/install appropriate hardware and software (assistive technologies) to be used by PWDs;
b. provide training, sensitization and awareness programmes on assistive technologies;
c. ensure that PWDs access ICT resources with ease;
d. promote research and development for ICT access for PWDs.
e. ensure websites and online portals meet the Web Content Accessibility Guidelines (WCAG)
f. ensure participation of PWDs in procurement of assistive technologies
g. ensure that online and audio-visual media content such videos have closed captioning

2.6 Use of ICT resources

Policy Statement

The Institute shall ensure proper use of ICT resources in communication, teaching, learning, research, consultancy and administration in support of the Institute's mandate.

Strategies

The Institute shall:

a. reserve the right to limit, restrict, cease or extend access to the use of its ICT resources;
b. permit commercial use of ICT resources for non-Institute related activities only under written authorisation from the Director;
c. ensure that ICT resources are not used for obtaining, possessing, transmitting, demonstrating, advertising or requesting of objectionable material.
d. protect the confidentiality of information and material submitted by staff, students and clients. The Institute shall bear no liability in the event of any improper disclosure.
e. safeguard the possibility of loss of information within the Institute's ICT facilities and services. Incase of any loss, the Institute shall not be liable to the user.
f. ensure that the use of ICT facilities and services is permitted on condition that it does not involve infringement of any patent or breach of any copyright. In the event of infringement or breach, the user shall bear the liability.
g. terminate access to the Institute's ICT resources when one ceases to be an enrolled student, a non- payroll associate, or an employee. Users are responsible for their information and must remove it or make arrangements for its retention prior to leaving the institute.
h. reserve the right to periodically check and monitor ICT facilities and services and reserve any other rights necessary to protect them.
i. personal devices joining the network shall have an up-to-date antivirus programme and licensed software.

Use of E-Mail

a. Staff and students shall be provided with email and communication facilities by the Institute.
b. The website, portal and email shall be used to broadcast official messages to staff, students and clients.
c. All users must display appropriate email etiquette and best practice when writing emails.
d. Email may be used for personal communication within appropriate limits.
e. Users shall explicitly recognize their responsibility for the content, dissemination and management of messages they send.
f. The Institute shall take no responsibility and provide no warranty against non-delivery or loss of files, messages, or data nor shall it accept any liability for consequential loss in the event of improper use or any other circumstances.
g. Email users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the institute or any unit of the Institute unless appropriately authorized to do so.
h. Systems Administrators shall establish and maintain a systematic process for recording, retention, and destruction of electronic mail messages and accompanying logs.
i. Incoming/outgoing email shall be screened for computer viruses and malicious codes.
j. Internal email address lists shall be properly maintained and protected from unauthorized access and modification.
k. Emails from suspicious sources should not be opened or forwarded and shall be reported to the ICT Office

2.7 Use of Social Media

Policy Statement

The use of social media in the Institute facilities by staff and all third parties shall be governed by a social media policy.

Strategies

a. Social networking sites shall not be accessed for personal use from the Institute's workstations during official working hours.
b. Political impartiality shall be upheld when engaging in the social media platforms in both personal or professional capacities.
c. No confidential or proprietary information about the Institute, its operations or its personnel shall be posted or shared in any social media sites.
d. Institute employees shall not post or share material that is, or might be construed as, threatening, harassing, bullying or discriminatory towards another employee or members of public.
e. Institute personnel shall not make any comment or post any material that might otherwise cause damage to the Institute's reputation or bring it into disrepute.

f. While using social media no Institute employee shall give the impression that the views they express are those of the Institute or imply that they are authorized to speak as a representative of the Institute.

g. No Institute employee shall impersonate another employee or contractor while using social media.

2.8 Network Management

Policy Statement

The Institute's LAN, WAN and associated telecommunications networks shall be designed to facilitate the exchange of information between connected ICT systems.

Strategies

a. The primary security controls shall be applied at the application level.

b. Data networks shall be managed in such a way as to prevent unauthorized logical and physical connection, and to detect unauthorized connections should this occur.

c. Information classified as Top Secret and above as well as Personnel Confidential records shall not be sent to a network printer without watch by an authorized person to safeguard its confidentiality during and after printing.

2.9 Classification of Information

Policy Statement

To ensure that information assets receive an appropriate level of protection, such information assets shall be classified to indicate the need, priorities, and degrees of sensitivity and criticality.

Strategies

a. The information classification system shall be used to define an appropriate set of protection levels, and to communicate the need for special handling measures.

b. The Institute shall identify data that is of a particular sensitive nature and its storage by establishing different access levels.

c. Information classified as Confidential and above shall be secured accordingly.

2.10 Third Party Services Management

Policy Statement

The Institute shall manage third party services while establishing relationships and bilateral responsibilities with qualified third party service providers.

Strategies

a. The Service Level Agreement shall explicitly outline the responsibilities of the Institute and the service provider.

b. All third-party service providers while undertaking the support and implementation of ICT equipment and systems shall be monitored and accompanied by technical staff with requisite knowledge to ensure the security of Institute systems is not compromised.

2.11 Security Risk Assessment and Auditing

Policy Statement

To evaluate the effectiveness and suitability of existing information systems and applications, the Institute shall conduct risk assessment and audit.

Strategies:

a. security risk assessments on information systems and production applications shall be performed annually.
b. a security risk assessment shall also be performed prior to major enhancements and changes associated with these systems or applications.
c. information systems shall be periodically audited by ICT Office to determine the minimum set of controls required to reduce risk to an acceptable level.
d. auditing of compliance of computer and network security policies shall be performed periodically by ICT Office.

2.12 Cyber Security Awareness

Policy Statement

To reduce on cyber threats and the potential impact of cyber-attacks, the Institute shall create awareness on cyber security.

Strategies

a. Users shall be provided with information security awareness tools to enhance awareness and education regarding the range of threats and appropriate safeguards that may result from sensitive data being acquired unlawfully, damaged or modified.
b. Third party contractors/consultants/ temporary personnel shall be given a brief overview or summary of information security policies prior to be being allowed to undertake any project within the Institute to avoid data loss in error or through negligence.
c. The ICT Office shall provide training to all authorized systems users to ensure that their use is both efficient and does not compromise information.
d. All information security personnel from the Institute shall be provided with periodic training as a priority to equip them with the right skills on the latest threats and information security techniques.

2.13 Skills development

Policy Statement

Training shall be conducted to provide new ICT skills, bridge skills gaps and sharpen existing ICT competencies to improve performance. This shall be executed in line with the Institute Human Resource Development policy.

Strategies

The Institute shall;

a. capacity build ICT staff to improve their technical knowledge as per Training Needs Assessment (TNA) and when need arises;
b. Ensure users are trained on the systems they use for their daily work;
c. Conduct trainings and capacity building of employees involved in operations, management and support of all newly deployed systems;
d. Induct new users to the deployed system;
e. Ensure availability of well-equipped ICT training computer labs.

2.14 Management and Maintenance

Policy Statement

ICT equipment shall be regularly maintained to ensure all Institute's systems run efficiently with minimal downtime.

Strategies

The Institute shall:

a. Provide technical support in servicing and maintaining Institute ICT equipment;
b. define and disseminate updated ICT equipment maintenance guidelines to all staff;
c. Undertake annual assessment to ensure compliance with set maintenance guidelines
d. Maintain an automated register of all ICT equipment acquired including records of manufacturer equipment warranty
e. Ensure all ICT equipment is situated within adequate operating environments
f. Ensure all replacements or upgrades of any ICT equipment is undertaken when need arises
g. Ensure outsourced maintenance services are carried out as per the agreed vendor Service Level Agreement for critical equipment
h. Ensure equipment such as multifunctional printers (MFP), air conditioners and high-end UPS are placed on maintenance contracts.
i. ICT office shall evaluate, procure and deploy appropriate network management applications to ensure uptime, security, efficiency and effectiveness of the network.
j. Any loss of ICT equipment shall be reported to the ICT office in line with ICT equipment loss guidelines.

Chapter Three: Institutional Framework

3.1 Introduction

The Institute management shall take full responsibility for implementation of this policy.

3.2 Management

The ICT Office together with ICT Steering Committee shall be responsible for day to day implementation of this policy.

3.3 ICT Office

The ICT Office shall be headed by the ICT Officer who shall report to the Office of the Director. The office shall comprise of a Systems Administrator, Network Administrator, Students Information Administrator and ICT Support Technicians.

3.3.1 Roles and Responsibilities of ICT Office

a. System administrator shall be responsible for setting up and maintaining the Dynamic Host Configuration Protocol (DHCP) server, Active Directory/domain controller (AD/DC) server, Domain Name System (DNS), mail server, Enterprise Resource Planning (ERP) and management systems, file servers, updating the website and backup & restore of all systems under their care.

b. Network Administrator shall be responsible for setting up, maintaining and monitoring the Institute network, firewall, CCTV system and backup & restoration of all systems under their care.

c. Students Information Administrator shall be responsible for handling all systems relating to students' affairs. These include emails, students' portal, e-learning management system, library management system, meals control system and backup & restore of all systems under their care.

d. ICT Support Technicians shall be responsible for handling ICT support issues from the Institute staff and clients.

3.4 ICT Steering Committee

The ICT Steering Committee shall support activities of the ICT Office and advise management on all ICT matters. The Committee shall comprise of members from the following departments:

a. A member of the Senior Management – Chairperson
b. ICT Officer - Secretary
c. Academic Registrar office
d. Internal Audit
e. Finance office
f. Supply Chain Management Office
g. One representative from the ICT office

3.4.1 Roles and Responsibilities of the ICT Steering Committee

a. Decides the overall level of ICT spending and how costs will be allocated
b. Aligns and approves the Institute's ICT architecture
c. Approves project plans and budgets, setting priorities and milestones
d. Acquires and assigns appropriate ICT resources
e. Ensures that projects continuously meet business requirements including re-evaluation of the business case
f. Monitors projects plan for delivery of expected value and desired outcomes, on time and within budget
g. Monitors resource and priority conflict between departments and ICT functions as well as between projects.
h. Makes recommendations and requests for changes to strategic plans (Priorities, funding, technology approaches and resources)
i. Communicates strategic goals to projects teams
j. Ensure equity in distribution of acquired ICT resources.

3.5 Dissemination of the Policy

ICT Steering Committee shall ensure dissemination as well as awareness creation of this policy. This policy shall be disseminated to all staff, students and stakeholders through the Institute website and organized forums.

4.0

Chapter Four: Monitoring and Evaluation

4.1 Monitoring and Evaluation

Policy statement

The Institute shall ensure continual improvement through monitoring and evaluation of ICT facilities and services.

ICT Office in partnership with the ICT Steering Committee shall be responsible for monitoring and evaluation of the implementation and compliance of this policy and where necessary shall take appropriate remedial measures as approved by the Institute management.

Strategies

a. Develop and implement a monitoring and evaluation plan.
b. carry out annual evaluation on the implementation of the policy;
c. define short, medium- and long-term interventions based on the outcomes of the monitoring and evaluation reports
d. Advise the institute on areas of improvement.

Chapter Five: Policy Review

5.1 Policy Review

This policy shall be reviewed after every three (3) years or when the Institute management may deem necessary to consider any relevant emerging issues and trends.