KNLS

Read. Know. Empower

kenya national library service

ICT POLICY

2019

FOREWORD

Implementation of ICT infrastructure and systems requires elaborate guiding framework to ensure compliance with legal and regulatory requirements, Value Creation, Proper Management and alignment to organizational business objectives. knls ICT policy aims at guiding the acquisition, deployment, use, maintenance and disposal of all ICT services and assets for efficient and effective service delivery. Knls ICT policy is aligned with the GoK ICT standards, knls Strategic Plan, ICT strategic plan 2018-2023 among other policy documents.

This knls ICT policy sets out explicit, single-minded and tenacious guidelines whose compliance will not only cement efficient, reliable and effective service delivery, but will result in prudent use of available resources in furthering new and innovative products and services. In equal measures and in line with ICT strategic plan 2018-2023, the policy will enforce effective ICT management that require deployment of the right technology in the right way and for the right reasons.

The board applauds all the participant in the development process of this Policy document whose varied and valuable contributions made this a successful endeavor. The board will continue to provide headship and sustenance in compliance and conformance with this policy and Government ICT standards.

Hon. Noah Katana Ngala, EGH
Chairman, knls Board

ACKNOWLEDGEMENT

ICT has become the lifeblood of humdrum processes in all organizations and knls is not an exception. In addition, organizations all over the world, knls included, are faced with the challenges of ICT security and drawing the line between acceptable and non-acceptable use of ICT. Legal acquiescence and compliance with set government and industry standards are key to any ICT function in public sector today. This knls ICT Policy document will provide guidelines for compliance, acceptable and secure use of ICT and associated technologies by knls employees, knls business partners and library users.

This knls ICT Policy document is an upshot of assembled input, expertise and wisdom from various staff, consultants and stakeholders. To you all, we are grateful. We acknowledge the development team members for their effective commitment, participation and involvement. We remain indebted the Board for leadership and support in the development of this Policy. We thank all other stakeholders for their invaluable contribution during the strategic planning process. We appreciate the Government of Kenya through the Ministry of ICT and ICT Authority for their guidance and Support.

To realize the intended benefits, knls commits to full implementation and compliance with the policy guidelines herein.

Richard Atuti, OGW

CEO/Director

TABLE OF CONTENT

ABBREVIATIONS & ACRONYMS

CCTV	Close Circuit Television
PCD	Personal Communication Device
ICT	Information and Communication Technology
ICTA	Information and Communication Technology Authority
SLA	Service Level Agreement
BCP	Business Continuity Plan
Knls	Kenya National Library Service
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
ISO	International Standard Organisation
UPS	Uninterruptible Power Supply
HOB	Head of branch
HOD	Head Of department

DEFINITIONS

ICT Infrastructure	ICT equipment, the network and any other installations that are in place to ensure ICT service availability
Assets	All applications and technologies that are owned, procured and/or managed.
Equipment	The necessary items for a particular purpose
Software	A program that allows access to computer hardware for purposes of processing data. System and software may be used interchangeably.
Hardware	Collection of physical parts of a computer
Stakeholders	A person, group or organization that has interest or concern in an organization
Intranet	A private service for collaboration that shares data and application resources accessible only in the organization by employees or authorized users
Data Center	An ICT facility where equipment including servers, network equipment, storage facilities are installed and operated to ensure they are protected from physical damage or tampering with an aim to ensure service availability.
Data	This is information that has been translated into a form that is more convenient to transmit or process.
Decommissioning	A systematic process of terminating obsolete ICT equipment, software and systems from day to day use upon lapse of their lifespan or when they no longer serve the intended purpose.
Users	Is a person who uses a computer or network service
Clean power	The is electrical power that has been regulated by passing it through a voltage regulator/stabilizer and is supplied to the ICT equipment through an Uninterruptible Power Supply.
Inappropriate Content	This is content that contravenes knls acceptable use policy and is culturally, socially or ethically inappropriate including sexually explicit material, racial bigotry, obscene, or discriminatory content.
Information Systems	These are computer hardware and software, telecommunications, databases and data warehouses, human resources, and procedures.

Information	Data that has been analyzed and summarized in a form that is easy to interpret and make conclusions from.
Governance	Establishment of policies, and continuous monitoring of their proper implementation, by the members of the governing body of an organization
Networks	A group of two or more computer systems linked together
Firewall	Network security system either hardware or software-based that uses rules to control incoming and outgoing network traffic
Access	Authorized entry to knls facilities and systems
Malware	Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system

1.0 INTRODUCTION

1.1 BACKGROUND

Kenya National Library Service (knls) is a statutory body of the Government of Kenya established by an Act of Parliament, Cap 225 of the Laws of Kenya in April 1965 with a mandate to develop, promote, establish and equip libraries in Kenya.

The strategic objective number two of knls Strategic Plan 2017 - 2022 is to upscale automation levels for enhanced access to services. knls is committed to provide Kenyan communities with high quality and accessible library and information services that the available resources will allow. Hence, availability of adequate and relevant information and communication technologies is an integral part of knls service delivery system.

This ICT Policy provides for guidance on ICT decisions to achieve the objectives of knls Board. Further, it identifies best practices for ICT in standardization of processes in expeditious service delivery. This policy shall ensure availability, confidentiality, security and integrity of ICT resources, which support operations of knls Board. This policy is guided by the knls Board Strategic Plan 2017 – 2022, knls, ICT Strategic Plan 2018 – 2023 and the GOK ICT Standards.

1.2 SCOPE

This Policy defines guides for acquisition, management and operation of ICT resource including infrastructure, systems and applications, devices and other related technologies.

1.3 OBJECTIVE

The overall objective of this policy is to enhance service delivery through optimization and leveraging use of ICT in knls services.

1.4 VISION

The model ICT function

1.5 MISSION

To leverage ICT in secure storage, access and sharing of information for enhanced service delivery.

1.6 VALUES

T - Technology driven: We will continually integrate technology in all our operations and service delivery

I – Innovation: We will embrace new ways, ideas and products to satisfy our customer needs

C - Customer focus: We will serve our customers with passion, integrity and professionalism

K - Knowledge based: We will continually review our services and products to support social economic Development

1.7 OWNERSHIP AND DISSEMINATION

This document is owned by knls Board and shall be disseminated through knls website, intranet, staff meetings and other fora.

1.8 LEGAL AND REGULATORY PROVISIONS

This policy has taken into consideration the following existing legal provisions among others: -

i. Act of Parliament, Cap 225 of the Laws of Kenya
ii. Public Procurement and Disposal Act
iii. Data Protection Bill 2018
iv. GOK ICT Standards
v. knls ISO Quality Systems Procedure
vi. knls HR Manual
vii. knls HR Access to Information Manual
viii. knls Innovation Policy

1.9 BROAD POLICY AREAS

This policy document addresses the following broad policy areas:

1) IT Governance
2) Change management
3) ICT Human Capital and Training Policy

2.0 ICT GOVERNANCE

2.1 ICT GOVERNANCE POLICY

2.1.1 Introduction

ICT governance is the processes that ensure effective and efficient use of IT in enabling an organization to achieve its goals. ICT Governance covers the culture, organization, policies and practices that provide oversight and transparency of ICT. For organizational investment in ICT to deliver full value, ICT has to be fully aligned to business strategies. The benefits of good IT risk management, oversight and clear communication not only reduces the cost and damage caused by ICT failures but also stimulates greater trust, teamwork and confidence in the use of ICT and the people trusted with ICT services.

2.1.2 Purpose

The purpose of this policy is to provide the organization with clear and concise guidelines on the management and the use of ICT resources.

2.1.3 Scope

This policy centers on ICT organization and governance focusing on five key areas:

a) Alignment that provides strategic direction of ICT business processes
b) Value Delivery to ensures ICT services attain maximum value
c) Risk Management to ascertain that IT business processes are in place and risks are managed
d) Resource management to give strategic direction for sourcing and use of ICT resources
e) Performance to ascertain compliance and achievement of ICT objectives

2.1.4 Application

This policy applies to the Board of Directors, the Management and staff of knls.

2.1.5 Policy Statement

This ICT governance policy shall be in accordance with GoK ICT Governance Standard and aims at providing strategic alignment of ICT services to the business objectives knls.

2.1.6 Policy Guidelines

2.1.6.1 Knls shall setup an ICT steering committee at boards level and in line with ICT governance standard to provide oversight matters to issues related to ICT.

2.1.6.2 knls shall ensure that there is enough capacity to manage ICT services and projects.

2.1.6.3 knls shall ensure that ICT function report directly to the CEO.

2.1.6.4 knls shall develop and properly disseminate ICT service charter for all ICT enabled services.

2.1.6.5 knls shall allocate adequate funds to support ICT services through the annual budget.

2.1.6.6 knls shall conduct and document customer satisfaction surveys on ICT enabled services annually for internal and external customers.

2.1.6.7 knls shall develop and sign service level agreement (SLA) with all ICT service providers to ensure reliability and availability of outsourced ICT services.

2.1.6.8 knls shall develop and implement quarterly preventive maintenance plans for ICT equipment.

2.1.6.9 knls shall ensure that ICT projects are conducted as per the GOK ICT project management standards.

2.1.6.10 knls shall acquire and install ICT help desk management system to handle all support requests from end users.

2.1.6.11 knls shall seek legal advice whenever engaging challenging, risky and complex contracts for ICT service provision.

2.1.7 Enforcement

The management through the head of ICT function shall ensure compliance to this policy.

2.2 CHANGE MANAGEMENT POLICY

2.2.1 Introduction

New systems can be highly disruptive to an organizational; well executed change management initiatives ensure smooth transitions to new work processes thus eliminating interruptions to organization operations.

2.2.2 Purpose

The purpose of this policy is to guide knls in instituting and undertaking change management in order to ensure that changes are carried out in a planned manner to minimize negative impact to services and customers.

2.2.3 Scope

This policy covers all changes in implementation of new ICT infrastructure, systems and related technologies

2.2.4 Application

This policy applies to all users, technical staff, service providers and management who are involved or are affected by the changes.

2.2.5 Policy Statement

Changes to configurations, systems, applications or equipment that affect the work of more than one person shall follow the appropriate ICT change management procedures to minimize adverse impacts of the changes to operations.

2.2.6 Policy Guidelines

2.2.6.1 All changes shall be initiated using a request for change (RFC) form submitted by process owners and approved by respective HOD/HOB. RFC form shall contain enough information to enable evaluation of the potential impacts, risks and benefits.

2.2.6.2 knls change management procedure shall include:

a) Change Classification based on the need and urgency.
b) Change evaluation taking into consideration the feasibility; human and physical resource requirements and costs; impact on service delivery; information security and risks.
c) Notification on the time, duration and services that could potentially be affected should be sent to all customers affected by the change.
d) A roll-back plan shall be developed and implemented before the change is carried out.
e) Changes shall be tested in a test environment before implementation.
f) The change shall be effected at a time that will minimize disruption to service delivery.
g) Users shall be notified on the results of the change once the changes are complete.
h) Users shall be taken through formal training on the new operational processes impacted by the change.
i) Users shall review and accept completion of the changes and readiness for productions; the review shall be documented.

2.2.7 Enforcement

knls shall ensure compliance to this policy; violation of this policy may be subjected to disciplinary actions as per HR manual, Public Service Code of Regulation and other relevant regulations.

3.0 ICT HUMAN CAPITAL AND TRAINING POLICY

3.1. Introduction

By investing in people through training knls will strive to harness the full potential of its ICT personnel for organizational needs and personal development.

3.2 Purpose

This policy will guide on skills needed in recruitment and retention of ICT officers; and ICT workforce training and Human Capital development.

3.3 Application

This policy applies to human resource department, ICT staff, non ICT staff and library users

3.4 Scope

The policy covers all ICT capacity building aspects including technical and end user training.

3.5 Policy statement

ICT training shall be conducted to provide new ICT skills; bridge any ICT skills gaps and sharpen the existing ICT competences for improved service delivery.

3.6 Policy Guidelines

3.6.1 knls shall ensure that ICT personnel recruitment processes are in line with the overall Government personnel policies and procedures

3.6.2 knls shall implement processes to ensure that the organization has an appropriately deployed ICT workforce that has the skills necessary to achieve organizational goals

3.6.3 All knls staff shall be inducted with appropriate ICT orientation when hired and ongoing training to maintain their knowledge, skills, abilities, internal controls and security awareness at the level required to achieve organizational goals.

3.6.4 knls shall take expedient actions regarding job changes, especially job terminations to ensure knowledge transfer needs to be arranged, responsibilities reassigned and access rights removed such that risks are minimized and continuity of the function is guaranteed

3.6.5 Each ICT professional shall have defined minimum ICT skills/qualifications to ensure that they have the knowledge to perform the ICT activities.

3.6.6 knls shall ensure there is a minimum ICT literacy, skill and competency for all staff. There shall be a program to upgrade the skills, qualifications, competencies of those employees who do not meet that minimum threshold.

3.6.7 ICT staff training shall include training on management skills and priority shall be given to professional courses.

3.6.8 knls will ensure ICT staff are accredited and certified in their areas of specialization.

3.6.9 Knls will ensure ICT staff are subscribed to ICT Membership to professional bodies and actively participate in seminar/workshops organized by the member institutions

3.6.10 ICT department shall be involved in the planning of ICT training activities for all levels of staff in knls and stakeholders

3.6.11 There shall be equity in ICT capacity development opportunities for all knls end users to ensure that development of competencies for improved service delivery is across the entire knls board.

3.6.12 A training manual shall be developed for end user and other stakeholders training programs to ensure that capacity building are harmonized

3.6.13 All ICT projects shall have a well-defined training plan.

3.6.14 knls shall ensure that ICT officers mandated to maintain or support software acquired are adequately trained.

3.6.15 Where a maintenance contract is in place, knls shall ensure that measures are put in place to enforce knowledge transfer to ICT officers by contractors and vendors for continuous support and maintenance of the system once the contract expires.

3.7 Enforcement

An appropriate and continuous improvement, monitoring and evaluation framework will be employed to assess the impact of the ICT capital and training investments.

4.0 ICT INFRASTRUCTURE MANAGEMENT

4.1 HARDWARE ACQUISITION AND DISPOSAL POLICY

4.1.1 Introduction

Hardware acquisition constitutes acquisition of physical computing equipment and resources used by knls staff, Library users and stakeholders. This policy provides guidelines to facilitate acquisition, management and disposal of all hardware assets within knls.

4.1.2 Purpose

This policy will provide guidance on the acquisition, usage, maintenance and disposal of all hardware assets within knls.

4.1.3 Scope

This policy covers acquisition of servers, desktops, laptops, printers, network equipment, CCTV, smart screens, baggage/walk through/handheld scanners, mobile devices, desktop peripherals and any other related ICT equipment.

4.1.4 Application

This policy applies to knls Board, staff, library users and stakeholders.

4.1.5 Policy Statement

This policy will guide knls in acquisition, maintenance and disposal of ICT hardware.

4.1.6 Policy Guidelines

4.1.6.1 Procurement of ICT equipment shall be channeled through the Head of ICT Department who shall be responsible for the preparation and issuance of all technical specifications for the equipment.

4.1.6.2 Personal Communication Devices (PCDs) shall be issued only to personnel with duties that require them when they are away from their normal work locations. Effective distribution of the various technological devices shall be coordinated with Senior Managers.

4.1.6.3 All ICT equipment procured, donated shall be required to meet industry and safety standards and comply with the procurement laws.

4.1.6.4 knls shall ensure all equipment are maintained in accordance with the manufacturer's instructions and knls ICT quality systems procedures

4.1.6.5 ICT Department shall ensure that all relevant information is transferred to the organization and securely erased from unserviceable and obsolete ICT equipment.

4.1.6.6 Any unserviceable and obsolete ICT equipment will be identified and be disposed in accordance with various method provided by the with the procurement laws.

4.1.7 Enforcement

knls shall ensure compliance with this policy. Any employee found to have violated this policy will be subject to disciplinary action as per the knls HR Manual, Public Service Code of Regulation and other relevant regulations.

4.2 NETWORK DEPLOYMENT AND MANAGEMENT POLICY

4.2.1 Introduction

This policy provides a framework for design, installation and management of all categories of ICT networks in knls including local areas networks, wide area networks and networ active devices .

4.2.2 Purpose

This policy will provide guidance in establishing the responsibility and authority for ownership, acquisition, and management of knls enterprise network infrastructure.

4.2.3 Scope

This policy covers network infrastructure at knls HQ datacenter and all branches

4.2.4 Application

This policy applies to knls Board, staff, Library users and stakeholders.

4.2.5 Policy Statement

This policy shall support different sets of business needs at diverse locations of knls. This policy shall conform to network architecture that adheres to GOK ICT Network Standard.

4.2.6 Policy Guidelines

4.2.6.1 knls shall Deploy a WAN interlinking national, county and other libraries.

4.2.6.2 knls shall deploy and maintain a high performance LAN infrastructure.

4.2.6.3 knls shall ensure sufficient internet bandwidth for all users.

4.2.6.4 knls shall ensure knls firewall and perimeter architecture are configured.

4.2.6.5 knls shall ensure that all systems and active devices are managed and connected.

4.2.6.6 knls shall deploy and maintain network monitoring and management tools to ensure availability and optimal performance of network hosts and services.

4.2.6.7 knls shall strive to provide shared infrastructure services.

4.2.6.8 knls shall provide secure and reliable wireless network access to all users

4.2.6.9 ICT department shall be involved in the planning, acquisition, maintenance, of on-going connectivity for all network devices to ensure the appropriate network design, interoperability of components and integrity of operation.

4.2.7 Enforcement

knls shall ensure compliance with this policy

4.3 BYOD POLICY

4.3.1 Introduction

knls promotes use of user devices in the environment for access to information. The policy aims to manage user access, privacy, permission, loss and damage

4.3.2 Purpose

The purpose of this policy is to provide guidelines to knls staff and library users on use of personally owned electronic devices within knls premises.

4.3.3 Scope

This policy is applicable to anyone using a non-knls owned device for example laptops, Personal Digital Assistants (PDAs), Smart phones, tablets and similar technologies, commonly known as BYOD, to access information and/or ICT services. This also includes visitors to knls.

4.3.4 Application

This policy applies to knls Board, staff, library users and contractors.

4.3.5 Policy statement

The policy provides knls Board, staff, library users and stakeholders with rules and guidelines on use of personal devices.

4.3.6 Policy Guidelines

4.3.6.1 It is the responsibility of the BYOD user to ensure they are aware and compliant with the Government's privacy and data protection, rules and regulations to understand the consequences of the loss of data.

4.3.6.2 ICT Department will support the connection to knls systems and accounts only where necessary. Users have a responsibility to learn how to use and manage their device effectively.

4.3.6.3 knls Board takes no responsibility for supporting, maintaining, repairing, insuring or otherwise funding employee/library user BYOD, or for any loss or damage resulting from support and advice provided.

4.3.6.4 Faults caused by user downloaded applications will not be rectified by ICT Department. Any application that causes security vulnerabilities will be denied access to knls systems/networks.

4.3.6.5 ICT Department shall assist in changing passwords to knls services only. All personal sites, such as social media sites and personal digital accounts shall have to be changed by the user.

4.3.6.6 knls shall provide guidance on software and malware issues, on a reasonable endeavors basis. knls shall not take responsibility to implement the remedial actions.

4.3.6.7 When using a BYOD for any purpose, users MUST maintain the security of knls information at all times which includes, but is not limited to viewing, accessing, storing or otherwise processing of data.

4.3.6.8 Users will be required to assist and support knls in carrying out its legal and operational obligations, including cooperating with ICT Security should it be necessary to access or inspect knls data stored on BYOD.

4.3.6.9 knls Board reserves the right to monitor, investigate, refuse, prevent or withdraw access to users and/or any BYOD or software where it considers that there is unacceptable security, or other risks, to its staff, students, business, reputation, systems or infrastructure.

4.3.6.10 ICT Department may instruct users to update or install software that allows device management or enables access to or obtain information from their BYOD.

4.3.6.11 Any BYOD found to have the manufacturer's security mechanisms circumvented, such as 'jailbreak' will not be supported and knls Board have the right to deny access to reduce the risk to the knls network.

4.3.6.12 BYOD will only be allowed to knls network once proof of surety that the connection of the said device will not lead to denial or degradation of service to other users.

4.3.7 Enforcement

An agreement containing BYOD acceptable user statements shall be signed by all employees, service providers and users clearly defining mutual responsibilities of knls and the signatory prior to connecting employee/contractor owned device to the Institution network/systems.

5.0 SYSTEMS AND APPLICATIONS

5.1 SOFTWARE ACQUISITION, DEPLOYMENT AND DECOMMISSIONING POLICY

5.1.1 Introduction

Software platform for knls acts as an enabler to accelerate automation services and improve productivity of library services. It is important to Identify the right software and vendor to undertake installation, customization, testing, training, commissioning and utilization.

5.1.2 Purpose

This policy shall provide guidance on the software acquisition, usage, maintenance and decommissioning.

5.1.3 Scope

This policy covers all software acquired and used by knls.

5.1.4 Application

This policy applies to knls Board, staff, Library users and stakeholders.

5.1.5 Policy Statement

This software policy will guide in acquisition, maintenance and disposal of ICT software.

5.1.6 Policy Guidelines

5.1.6.1 Acquisition of the software shall be done with consultation and coordination of ICT department and user departments who shall be responsible in the development of technical and business specification for the software.

5.1.6.2 knls shall ensure all licenses for software upon acquisition are duly registered and subsequently renewed.

5.1.6.3 Software shall only be installed by authorized personnel.

5.1.6.4 Sectional Heads Shall identify the set of software per user groups for deployment to the end user computing device.

5.1.6.5 The software development process shall be approved with relevant plans and adopt a project management approach as stipulated in GoK ICT governance standard on project management subdomain.

5.1.6.6 In-house developed, outsourced, commercial, off-shelf and open source software acquisition shall conform to GoK ICT systems and application standards.

5.1.6.7 All Software programs shall be covered by copyrights and a license is required for their use to enable installation, upgrades, updates, software patching and licensing.

5.1.6.8 Application software, system software and application development shall be decommissioned at the end of the life in consideration of the Information security policy as per approvals and plans.

5.1.6.9 All traces of the data contained on computer equipment must be removed and destroyed prior to decommissioning.

5.1.7 Enforcement

knls shall ensure compliance with this policy. Employees who violates this policy shall be subject to disciplinary action as per the knls HR Manual. Public Service Code of Regulation and other relevant regulations.

5.2 WEBSITE MANAGEMENT POLICY

5.2.1 Introduction

knls website is a major information resource for both internal and external customers. knls shall put in place measures to promote its proper management and acceptable use.

5.2.2 Purpose

The purpose of this policy is to guide the design, development, maintenance and management of cohesive and consistent user friendly website.

5.2.3 Scope

This policy governs web-based applications and documents made available via the knls domain knls.ac.ke and its sub domains.

5.2.4 Application

This policy is applicable to all web pages hosted on the knls domain or directly associated with the knls website.

5.2.5 Policy Statement

knls website shall provide accurate, useful and timely information on all aspects of service provision.

5.2.6 Policy Guidelines

5.2.6.1 Knls shall establish a website management committee reporting to the CEO. The committee membership shall comprise:

1. Head of Corporate Communication (Chair)
2. Head of ICT (Secretary)

3. Selected heads of department

5.2.6.2 The design of all web pages shall conform to the technical and design requirements developed by the website management committee.

5.2.6.3 knls shall ensure websites are designed with consistent layout, usability, inter-operability.

5.2.6.4 knls shall ensure that websites and portals display in a manner that is consistent with the dignity and authority of the Government of Kenya and which is attractive and branded so that it is easily recognizable and usable by citizens.

5.2.6.5 knls shall host websites securely.

5.2.6.6 knls shall ensure that all web pages shall provide navigational links that appear and behave in a consistent fashion. The web pages shall provide any additional information when linking to resources or services that require a plugin or separate application.

5.2.6.7 knls website shall not be used for commercial purposes that are not related to knls mandate.

5.2.6.8 Knls website shall be designed, managed and maintained in accordance to the GoK ICT standards.

5.2.7 Enforcement

knls shall ensure compliance to this policy; violation of this policy may be subjected to disciplinary actions as per HR manual, Public Service Code of Regulation and other relevant regulations.

5.3 SOCIAL MEDIA POLICY

5.3.1 Introduction

Social media is a free promotional tool that allows employees to share work-related multi-media information on their personal and official social media channels. On the other hand, it is often misused and hence the need to regulate these communications without stifling them.

5.3.2 Purpose

This policy provides guidance for employee's use of social media.

5.3.3 Scope

This policy covers use of blogs, wikis, microblogs, message boards, chat rooms, electronic newsletters, online forums, social networking sites, and other sites and services that permit users to share information with others in a synchronous manner

5.3.4 Policy Statement

Knls shall ensure appropriate use and management of social media applications.

5.3.5 Application

This policy applies to all staff

5.3.6 Policy Guidelines

The following principles apply to professional use of social media on behalf of knls and personal use of social media when referencing knls.

5.3.6.1 Knls shall conduct and document a risk analysis prior to authorizing and enabling Internet access to Social Media websites.

5.3.6.2 Knls shall conduct and document this risk analysis and retain it for a minimum of two years upon which it must be revised.

5.3.6.3 Staff shall connect to, and exchange information with only those social media websites that have been authorized by knls management in accordance with this policy and other Government policies.

5.3.6.4 Staff shall not post or release proprietary, confidential, sensitive, personally identifiable information or other Government intellectual property on Social Media websites

5.3.6.5 Staff shall not speak in Social Media websites or other online forums on behalf of knls unless specifically authorized by knls Management.

5.3.6.6 Staff who are authorized to speak on behalf of knls shall identify themselves by full name, title, knls contact information; when posting or exchanging information on Social Media forums, and shall address issues only within the scope of their specific authorization.

5.3.6.7 Staff who are not authorized to speak on behalf of knls shall clarify that the information is being presented on their own behalf and that it does not represent the position of knls.

5.3.6.8 Staff shall not utilize tools or techniques to spoof, masquerade, or assume any identity or credentials except for legitimate law enforcement purposes.

5.3.6.9 Staff shall avoid mixing their professional information with their personal information.

5.3.6.10 Staff shall not use their work password on Social Media web sites.

5.3.6.11 Social media sites not owned or managed by knls must not be used as official delivery platform for information and services

5.3.7 Enforcement

knls shall ensure compliance to this policy; violation of this policy may be subjected to disciplinary actions as per HR manual, Public Service Code of Regulation and other relevant regulations.

5.4 EMAIL POLICY

5.4.1 Introduction

Email service is a key communications tool in knls. knls, in collaboration with Google, provides electronic mail and communication services to its staff. These services are locally hosted on the Google environment, located in the cloud, and provide a convenient solution to store or share information over the Internet.

5.4.2 Purpose

The purpose of this policy is to guide on appropriate use of the email service within knls facilities.

5.4.3 Scope

This policy covers use of any email sent from knls email address and applies to all staff and any agents operating on behalf of knls.

5.4.4 Application

This policy applies to all employees, service providers, trainers, training institutions and other stakeholders operating on behalf of knls.

5.4.5 Policy statement

It is a policy of knls that all staff must observe the guidelines outlined in this policy to ensure the proper use of the organization's electronic communication infrastructure system.

5.4.6 Policy Guidelines

5.4.6.1 All staff shall be facilitated with a knls email account in the format of firstname.lastname@knls.ac.ke. Staff email account shall belong to one or more email groups.

5.4.6.2 Staff shall not block, mark as spam, blacklist other users within knls domain.

5.4.6.3 knls email account shall be used primarily for knls business related purposes; personal communication is permitted on a limited basis, but non-knls related commercial uses are prohibited.

5.4.6.4 All use of email must be consistent with ICT Acceptable Use policy, network security policy and other policies and procedures of ethical conduct, safety and compliance with applicable laws.

5.4.6.5 All correspondences and circulars sent, received, forwarded or other shared on knls individual staff or group emails shall be taken as duly and officially communicated.

5.4.6.6 knls email shall be guided and used in accordance to Acceptable Use Policy. Sending, forwarding or otherwise transfer of inciting and offensive emails constitutes unacceptable use and is prohibited. Sending chain letters, press releases, joke emails or other junk-mail of any kind is prohibited.

5.4.6.7 Users shall take the same care in drafting an email as they would for any other communication. The following best practices are encouraged

a) Consider using attachments to communicate lengthy emails
b) Write well-structured emails and use short, descriptive subjects and straight to the point sentences.
c) Signatures must include your name, job title and name of the department.
d) knls email disclaimer shall be added underneath your signature
e) Users must spell check all mails prior to transmission.
f) Do not write emails in capitals.

5.4.6.8 All email will be retained for a period of 7 years after which the email shall be removed from the system.

5.4.7 Enforcement

knls shall ensure compliance to this policy; violation of this policy may be subjected to disciplinary actions as per HR manual, Public Service Code of Regulation and other relevant regulations.

6.0 ELECTRONIC RECORDS MANAGEMENT POLICY

6.1 Introduction

The growing need for access to information has informed the need for establishing policies on managing electronic records. The establishment of an electronic records management system will enhance service delivery through speedy access to information. Electronic records for knls will include data or communication generated by knls computer software and systems and stored in databases.

6.2 Purpose

The purpose of this policy is to effectively manage electronic records and improve both internal efficiency and overall organizational goals.

6.3 Scope

This policy applies to all electronic records created, received and managed by the knls staff.

6.4 Application

This policy shall apply to the knls staff at the headquarters and regional branches.

6.5 Policy Statement

knls shall commit to use electronic systems in the form of its Electronic Document and Records Management System for the storage of records over time. This system will be one of the knls' primary systems used for the storage of digitized documents to ensure their authenticity and reliability.

6.6 Policy Guidelines

6.6.1 knls shall deploy Electronic Record Management Systems to create, maintain, disseminate and administer electronic records

6.6.2 The Electronic Record Management Systems shall have adequate system controls, such as audit trails, the routine testing of system hardware and software, and procedures for measuring the accuracy of data input and output.

6.6.3 knls shall digitize records for better management

6.6.4 Knls shall protect e-records to enable their accurate and ready retrieval throughout their retention period

6.6.5 Where sensitive information is to be exchanged through the use of voice, fax, video and data communication facilities, precautions shall be taken to ensure that the confidentiality and integrity of the information is protected.

6.6.6 Data and information shall be categorized and classified according to their purpose and needs

6.6.7 knls shall adopt and use records retention and disposal schedules in compliance with the Kenya National Archives and Documentation Centre standards and guidelines.

6.7 Enforcement

Quarterly checks will be carried out by ICT Departmental to ensure policy is being applied. These checks and any remedial action taken shall be recorded. Violation this policy may be subject to disciplinary action up to and including denial of access, legal penalties, and/or dismissal in line with the HR manual. Any employee aware of any violation of this policy is required to report it to their supervisor or other authorized representative.

7.0 ICT SECURITY

7.1 PHYSICAL AND ENVIRONMENTAL SECURITY POLICY

7.1.1 Introduction

Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to knls ICT resources. Controls shall also be adopted to minimize the risk of potential environmental threats to the information processing facilities and other ICT facilities.

7.1.2 Purpose

This policy aims to prevent unauthorized physical access to or interference with information and information systems.

7.1.3 Scope

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

7.1.4 Application

This policy applies to all employees and all users accessing knls systems and applications

7.1.5 Policy Statement

It is the Board's duty to protect ICT areas of critical and sensitive information processing facilities to ensure confidentiality, integrity and availability of data and information.

7.1.6 Policy Guidelines

7.1.6.1 knls shall have multifactor identification mechanisms; biometrics, physical locks for the designated areas and having only authorized personnel accessing the secured areas.

7.1.6.2 knls shall ensure ICT facilities are built to physical and environmental industry standards.

7.1.6.3 knls shall ensure that access rights and access to areas where information is processed or stored shall be restricted to authorized individuals only.

7.1.6.4 knls shall ensure user authentication to restricted areas using access codes and tags.

7.1.6.5 Access rights to secure areas shall be reviewed, updated and/or revoked as and when necessary.

7.1.6.6 Data backup equipment shall be stored in a remote locked fireproof area. An automatic daily backup shall be done on the dedicated server. The backup shall be tested to ensure it can be restored if need be.

7.1.6.7 Knls shall ensure installation of clean power to protect ICT equipment from damage.

7.1.6.8 All ICT equipment shall be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.

7.1.6.9 Installation, disconnection, modification or relocation of ICT equipment shall only be performed by ICT authorized personnel.

7.1.7 Enforcement

Violation this policy may be subject to disciplinary action up to and including denial of access, legal penalties, and/or dismissal in line with the HR manual.

7.2 NETWORK SECURITY POLICY

7.2.1 Introduction

knls has a large and complex ICT infrastructure. The foundation of this structure is the Data and Communications Network which is facilitated and supported by many types of hardware including extensive cabling and supporting systems installed throughout the branch libraries and offices.

knls relies heavily on its Data and Communications Network infrastructure to carry out its functions and activities, communicate and provide internet access.

7.2.2 Purpose

The purpose of this policy is to ensure the security, integrity and availability of knls' Data and Communications Network and to establish professional good working practices and procedures.

7.2.3 Scope

The scope of this policy extends to all administration, installation and configuration of knls Data and Communications Network equipment and associated systems which form part of knls ICT infrastructure and which falls under the responsibility the ICT department. This policy must be undertaken in line with all existing GoK ICT Standards.

7.2.4 Policy Statement

Knls Data and Communications Network equipment is maintained and installed across all branch libraries and offices. Information processing facilities houses most of the Data and Communications Network equipment and serves as the main access area to knls ICT Infrastructure.

7.2.5 Policy Guidelines

7.2.5.1 All devices should be configured using strong administrative controls and passwords.

7.2.5.2 There shall be effective and properly configured firewalls, network separation and network monitoring tool to ease network management and deter network security breaches.

7.2.5.3 knls shall ensure confidentiality and integrity of data passing over public networks or over wireless networks to protect the connected systems and applications by having encryption mechanisms in place.

7.2.5.4 All devices shall be set up with a "least privilege necessary" model, whereby access is provided only to employees who require it to do their jobs.

7.2.5.5 Data on transit within knls systems shall be secured through encryption protocols as defined by industry best practices

7.2.5.6 Knls shall develop and ensure that a detailed cyber security plan to guide on best practices on prevention of cybercrime

7.2.5.7 knls shall block access to internet websites and protocols that are deemed inappropriate.

7.2.5.8 Access to Internet services shall be granted based on user needs. Users shall be required to responsibly use internet when granted access.

7.2.5.9 Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

7.2.5.10 Power cables should be segregated from communications cables to prevent interference.

7.2.5.11 Cables and equipment shall be clearly marked to minimize handling errors such as accidental patching of wrong network cables. A documented patch list shall be used to reduce the possibility of errors.

7.2.6 Enforcements

knls will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, Network monitoring, internal and external audits.

7.3 ICT ASSETS MANAGEMENT POLICY

7.3.1 Introduction

Asset management is the process of receiving, tagging, documenting, and eventually disposing of equipment. It is critically important for knls to maintain an up to date inventory and asset controls to ensure ICT equipment locations and dispositions are well known. Lost or stolen equipment often contains sensitive data. Proper asset management procedures and protocols provide documentation that aid in recovery, replacement, criminal, and insurance activities.

7.3.2 Purpose

This policy shall provide guidance on procedures and protocols supporting effective organizational asset management specifically focused on electronic devices.

7.3.3 Scope

This covers all knls ICT assets and related equipment.

7.3.4 Application

This policy applies to knls board, staff.

7.3.5 Policy Statement

This policy will guide knls in managing knls ICT assets.

7.3.6 Policy Guidelines

7.3.6.1 knls shall implement and maintain accurate, up to date, and consistent inventory of ICT assets.

7.3.6.2 knls shall undertake periodic review, access restrictions and classifications to sensitive assets, taking into account applicable access control policies.

7.3.6.3 All ICT assets shall be assigned to individual user or to a department who will be held responsible for their care and security at all times.

7.3.6.4 knls staff shall not be issued with more than one asset of the same type for similar purpose. All ICT assets that are no longer in use must be returned to ICT department for re-deployment.

7.3.6.5 All employees and external party users shall return/surrender all of the knls assets in their possession upon separation from knls Board. Where a user has knowledge that is important to ongoing operations, that information shall be documented and transferred to the knls.

7.3.6.6 knls Board shall ensure revaluation of all ICT assets after the depreciation period of 3 years and give the assets a new value to include into the accounting books.

7.3.6.7 Users must always contact ICT if they need to move, re-assign or return assigned ICT asset. Movement of assets assigned to employees when teleworking shall have authorized by Section Heads.

7.3.6.8 In order to ensure the confidentiality of information, any ICT asset that has been used to process or store sensitive information will be wiped before being re-issued and must go through a physical disposal and destruction process at the end of its useful life.

7.3.7 Enforcement

Regular audits will be carried out to ensure that assets are not being irregularly moved or transferred. Staff and visitors have a responsibility to ensure that they comply with this policy and its associated

procedures. Failure to comply with any aspect of this policy will be dealt with in accordance with the knls Disciplinary Procedure for staff.

7.4 LOGICAL SECURITY POLICY

7.4.1 Introduction

Logical security consists of software safeguards for knls system, including user identification, authentication, access rights and level. Logical access control protects ICT systems and data by verifying and validating authenticated users, authorized user access to ICT systems and data, and restricting transactions; read, write, execute, delete according to the user' authorization level.

7.4.2 Scope

This policy area covers access control policies for the identification, authentication, authorization and accountability to ensure the availability, integrity, and confidentiality of data in knls systems and applications.

7.4.3 Application

This policy applies to all staff and stakeholders with access to knls systems and applications.

7.4.4 Purpose

Logical security measures are meant to ensure that only authorized users are able to access information

7.4.5 Policy Statement

The Board will ensure that access to specific information or data is based on who is assigned access rights and privileges.

7.3.6 Policy Guidelines

7.3.6.1 Access rights and privileges to information systems and applications shall be assigned based on user's roles and responsibilities on the respective systems.

7.3.6.2 The process for managing user accounts shall be very strict where each staff will be held responsible for the actions taken with the user account given.

7.3.6.3 The competences of users with privileged access rights shall be reviewed regularly in order to verify if they are in line with their duties.

7.3.6.4 All users shall be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection.

7.3.6.5 Computers and terminals shall be automatically left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism when unattended and shall be protected by key locks, passwords or other controls when not in use.

7.3.6.6 The competences of users with privileged access rights shall be reviewed regularly in order to verify if they are in line with their duties.

7.3.7 Enforcement

knls shall ensure compliance to this policy; violation of this policy may be subjected to disciplinary actions as per HR manual, Public Service Code of Regulation and other relevant regulations.

7.5 MALWARE SECURITY POLICY

7.5.1 Introduction

The number of computer security incidents related to malware and viruses and the resulting cost of business disruption and service restoration continue to escalate. Implementing antimalware and antivirus systems must be done to reduce risks and manage knls computing environment.

7.5.2 Purpose

The purpose of this Anti - Malware Control is to provide exemplar guidance in line with knls best practice for the implementation of an organization wide Malware Policy.

7.5.3 Application

This policy applies to all staff and stakeholders with access to knls systems and applications.

7.5.4 Scope

This covers all forms of malware such as viruses, rootkits, worms and trojans that can cause disruption to the systems and applications

7.5.5 Policy statement

The Board will ensure that approved and maintained licensed anti-virus and Anti Malware software from known and trusted sources is deployed.

7.5.6 Policy Guidelines

7.5.6.1 All knls computers and computing devices shall run on the knls approved, updated and licensed anti-malware software.

7.5.6.2 Any device that connects to the knls network must have a current antivirus installed and running at all times. The antivirus software must be configured to automatically clean and remove an infected

file or to quarantine the infected file if automatic cleaning is not possible. The antivirus software must be configured to automatically update itself on a regular basis. Scans for viruses on the device must occur without user intervention on a regular basis. On systems where this is not possible, users are responsible for regularly initiating the scan and updating the software to protect against the latest threats.

7.5.6.3 All knls-issued computers must use the antivirus software installed and configured by ICT department. Users are prohibited from disabling or tampering with the installed antivirus software.

7.5.6.4 When a computer system is determined to be infected with a virus or other malicious software that system may be blocked and removed from the knls network until the threat is neutralized.

7.5.6.5 All e-mail inbound to knls shall be scanned for viruses, malware and spam. E-mail that poses a risk to the knls is blocked. No security software is 100% effective, however, all users must exercise appropriate caution when opening external websites, e-mails or attachments.

7.5.6.6 In case of an attack beyond knls control, knls shall seek technical assistance from relevant government agencies.

7.5.7 Enforcement

knls shall ensure compliance to this policy; violation of this policy may be subjected to disciplinary actions as per HR manual, Public Service Code of Regulation and other relevant regulations.

7.6 PASSWORD SECURITY POLICY

7.6.1 Introduction

Passwords are the entry point to all ICT resources. Protecting access to resources is pivotal in ensuring that systems remain confidential, available and with integrity.

7.6.2 Purpose

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

7.6.3 Scope

The scope of this policy includes all personnel who have or are responsible for an account on any knls information system that resides on knls network, has access to knls network or stores any non-public knls information

7.6.4 Application

This policy applies to all user accounts provided by knls and all knls employees and all ICT service providers that login to knls information systems and network

7.6.5 Policy Statement

An important aspect of computer security is the safeguarding of personal and confidential information of all individuals and organizations affiliated with knls. Properly chosen passwords by knls system users will assist in the control of access to systems and data.

7.6.6 Policy Guidelines

7.6.6.1 Passwords shall have a minimum of 10 characters with a mix of alphanumeric and special characters; if a particular system will not support 10 character passwords, then the maximum number of characters allowed by that system shall be used.

7.6.6.2 Passwords shall be kept confidential and shall not consist of well-known or publicly posted identification information.

7.6.6.3 Users will be prohibited from re-using the last 5 previously used passwords. The username and password(s) used for your knls accounts should never be used for any other non-knls accounts and services.

7.6.6.4 Passwords shall be memorized and never written down or recorded along with corresponding account information or usernames

7.6.6.5 Passwords shall not be transferred or shared with others.

7.6.6.6 Systems shall not be configured to allow user login without a password. System administrators shall harden their systems to deter password cracking by using reasonable methods to mitigate “brute force” password attacks. System administrators shall not use default passwords for administrative accounts.

7.6.6.7 Users are required to change their initial/default passwords at the first log on and thereafter recommended change after every 3 months or immediately in case an account or password is suspected to have been compromised.

7.6.6.8 Failed password attempts should be limited to between 3 following which an account should lock out. Accounts should only be reset by an independent authority or reset automatically after a period sufficient to prevent a brute force attack.

7.6.6 Enforcement

Users shall exercise care to safeguard ICT equipment assigned to them and will be held accountable for any loss or damage that may result from negligence.

7.7 HUMAN RESOURCE SECURITY

7.7.1 Introduction

The Board holds large amounts of personal and restricted information. Information security is very important to help protect the interests and confidentiality of the organization. Information security cannot be achieved by technical means alone. Information security must also be enforced and applied by people, and this policy addresses security issues related to people.

7.7.2 Purpose

This policy ensures that staff, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, prior to employment or engagement.

7.7.3 Policy Statement

knls shall perform checks to ensure that the individual user is suitable for access to the knls Information Systems and information in these systems.

7.7.4 Application

This policy applies to all knls staff, contractors and third party service providers.

7.7.5 Scope

This policy covers access to the organization's information systems or information by staff or any third party like contractors and service providers.

7.7.6 Policy Guidelines

7.7.6.1 All new employees shall be subjected to screening and, where required, other screening to meet any contractual requirements.

7.7.6.2 All users of information assets must be given Security Awareness Training that shall detail the Users' responsibilities and address best practices for satisfying those responsibilities.

7.7.6.3 The access rights of all staff, contractors and third party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.

7.7.6.4 When an individual is hired for a specific information security role, knls shall make sure that the candidate has the necessary competence to perform the security role and can be trusted to take on the role.

7.7.7 Enforcement

Any employee found to have violated this policy shall be subjected to disciplinary action in line with the knls HR Policy, public service Code of Regulations and other relevant legislation.

7.8 ACCEPTABLE USE POLICY

7.8.1 Introduction

knls avails ICT equipment and services to its staff, library patrons and general public to further achievement of its mandate and in line with mission and vision. The use of these facilities constitutes acceptance of this policy and is subject to limitations and guideline provided by this policy.

7.8.2 Purpose

This Acceptable Use Policy is intended to provide a framework for acceptable and unacceptable use of knls ICT equipment.

7.8.3 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at knls, including all personnel affiliated with third parties. This policy applies to all ICT equipment that is owned or leased by the organization.

7.8.4 Application

This policy applies to all knls staff

7.8.5 Policy statement

Access to computers, computing systems, and networks owned by knls is a privilege which imposes certain responsibilities and obligations on users. Use of these resources is subject to knls policies and regulations; All users of these resources must comply with specific policies and guidelines governing their use, and act responsibly while using shared computing and network resources.

7.8.6 Policy Guidelines

7.8.6.1 The electronic resources shall be used for the purpose for which they are intended and in compliance will all knls ICT policy guidelines.

7.8.6.2 Staff and users must respect the rights, privacy and property of others.

7.8.6.3 Staff and users must adhere to the confidentiality rules governing the use of passwords and accounts, details of which must not be shared.

7.8.6.4 While using knls network to access other networks, any abuses against such networks will be regarded as an unacceptable use of the network.

7.8.6.5 knls networks may be used for incidental personal purposes provided that:

a) The purposes are of a private nature, not for financial gain and does not contravene any other policies;

b) such use does not cause noticeable or unavoidable cost to knls

c) Such use does not inappropriately interfere with the official business of knls

7.8.6.6 knls network shall not be used for the following activities

7.8.6.7 The creation, dissemination, storage and display of obscene or pornographic material, hate literature, materials that promote criminal activities, defamatory materials or materials likely to cause offence to others.

7.8.6.8 The creation, dissemination, storage and display of any data that is illegal including, but not limited to, Statutes and Regulations of the organization

7.8.6.9 The downloading, storage and disseminating of copyrighted materials including software and all forms of electronic data without the permission of the holder of the copyright.

7.8.6.10 Deliberate interference with or gaining illegal access to user accounts and data including viewing, modifying, destroying or corrupting the data belonging to other users is unacceptable

7.8.6.11 knls network shall not be used for commercial work

7.8.6.12 Unauthorized connection of monitoring devices/ equipment to the knls ICT infrastructure which could result in the violation of knls policy, applicable licenses or contracts constitutes inappropriate use. This includes but is not limited to the attachment of any electronic device to the computing and networking facilities for the purpose of monitoring data, packets, signals or other information.

7.8.6.13 Misusing, disclosing without proper authorization, or altering information is prohibited and should be done in line to knls access to information manual.

7.8.6.14 Copyrighted material should not be distributed, copied or published in any form without consent of the originator and any copyright violation or infringement rests solely on the user.

7.8.6.15 Staff or any other user has no rights of privacy in their use of the Internet service provided by the knls.

7.8.7 Enforcement

Any employee found to have violated this policy shall be subjected to disciplinary action in line with knls HR Policy.

8.0 BUSINESS CONTINUITY POLICY

8.1 Introduction

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

8.2 Purpose

The purpose of this policy is to preserve the confidentiality, Integrity, and availability of knls Data and information for business continuity.

8.3 Scope

This policy addresses risks, backup, business continuity and restore aspects of knls data and I Information.

8.4 Application

This policy applies to knls staff, contractors, service providers and consultants who process and/or store board data.

8.5 Policy statement

The policy provides knls Board and staff

8.6 Policy Guidelines

8.6.1 knls Board shall identify and evaluate ICT risks and provide mitigation measures.

8.6.2 knls Board will ensure thorough and periodic review of all ICT related risks is undertaken, a dedicated ICT risk management mechanism needs shall be established.

8.6.3 The ICT Department shall ensure full or differential backup is done in line with knls ISO quality systems procedure with Accurate and complete records of the backup copies and documented restoration procedures produced

8.6.4 Backup information shall be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site

8.6.5 The backups shall be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site.

8.6.6 Knls are required to back up their data on the google drive platform in consultation with ICT department.

8.6.7 The knls Board shall ensure adequate backup facilities are provided.

8.6.8 Knls Board shall develop a Disaster recovery plan to enable business continuity.

8.6.9 Backup media shall be regularly tested to ensure that they can be relied upon for emergency use when necessary; this shall be combined with a test of the restoration procedures and checked against the restoration time required. Testing the ability to restore backed-up data shall be performed onto dedicated test media, not by overwriting the original media in case the backup or restoration process fails and causes irreparable data damage or loss

8.6.10 In situations where confidentiality is of importance, backups shall be protected by means of encryption

8.6.11 Backup arrangements for individual systems and services shall be regularly tested to ensure that they meet the requirements of business continuity plans. In the case of critical systems and services, backup arrangements should cover all systems information, applications and data necessary to recover the complete system in the event of a disaster.

8.6.12 Knls shall optimize data processes, access, storage and management in line with ICT strategic plan 2018-2023

8.7 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action as per knls HR manual.

9.0 EMERGING TECHNOLOGIES AND INNOVATION POLICY

9.1 Introduction

Innovation has become a crucial driver of an organization's growth, sustainability, efficiency and competitiveness. knls recognizes the need to provide an enabling environment to foster innovations and enhance their contribution to national development.

Emerging technologies are technologies whose development, practical applications, or both are still largely unrealized, such that they are figuratively emerging into prominence from a background of nonexistence or obscurity. knls will remain cognizant and duly consider such technologies to advance and improve its service delivery.

9.2 Purpose

Innovation in organizations can be stifled by lack of adequate framework under which to operate. The purpose of this policy is to ensure that the innovation process is done in an orderly manner for knls to achieve maximum benefits

9.3 Application

This policy applies to all knls staff

9.4 Scope

The policy covers all ICT innovations

9.5 Policy statement

Fostering innovations will strengthen knls capability to generate, transfer, and apply technologies; and ensure sustainable utilization of the organizations resources for the realization of knls development objectives

9.6 Policy Guidelines

9.6.1 knls shall create a conducive environment to promote research and development as well as innovation initiatives within the organization

9.6.2 All employees shall be encouraged to find and apply innovative ICT solutions to improve service delivery. knls shall endeavor to compensate employees that shall innovate and improve knls standing in line with overall knls innovation policy

9.6.3 Knls shall conduct regular scan emerging technologies with a view of incubating and adopting them for operationalization.

9.6.4 knls shall establish a resource center for ICT research and innovation. The resource center shall manage knowledge through databases and online resources to spur innovation.

9.6.5 knls shall implement and endeavor to patent the results of the innovation process.

9.7 Enforcement

knls shall ensure compliance to this policy; violation of this policy may be subjected to disciplinary actions as per HR manual, Public Service Code of Regulation and other relevant regulations.

10.0 MONITORING AND EVALUATION

All ICT resources are the property of KNLS board. The board therefore reserves the right to audit and monitor these resources to ensure compliance with this policy. The use of ICT Resources is not considered private but monitoring of the ICT systems activities will be carried out in a manner that respects the rights and legitimate interests of those concerned.

Users of KNLS board ICT systems should be aware that their activities can be monitored. In order to maintain their privacy, users of the KNLS board's ICT resources should avoid storing information on the systems that they consider private. By using the board's ICT systems, users expressly consent to the monitoring of all their activities within the board's ICT systems.

During the implementation of this policy, the board 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, Internal Audit, Planning and Human Resource Departments

11.0 APPENDICES

Knls ICT department Organogram To include ICT structure, current status of ICT and future outlook (Action: Alex)