REPUBLIC OF KENYA

COUNCIL OF LEGAL EDUCATION

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY

2024

COPYRIGHT

TABLE OF CONTENT

TABLE OF CONTENT

FOREWORD

The world economy is experiencing the impact of rapid globalization, the emerging and dynamic information age comprising new Information and Communication Technology (ICT), which is bringing about a new global economic order dominated by information and knowledge-based economies.

The Council of Legal Education (CLE) has embraced Information Communication Technology to meet service delivery objectives of improving services and increasing productivity through ICT investment. Over the recent years, CLE's operations have increasingly depended on ICT whose capacity has tremendously grown following successful digitization and automation of key services.

The adoption and use of ICT has since created a considerable amount of investment in Information Systems to enhance the processing, transmission, and storage of information in CLE. All these developments require a comprehensive policy framework to guide ICT adoption, acquisition, use, and governance within the institution.

The implementation of the Policy will enable CLE to provide necessary and critical governance tools on ICT in a bid to ensure the effective execution of its mandate through the adoption of the relevant latest technology. It will also help the staff to effectively participate in a rapidly changing world where work and other activities are increasingly transformed. I hope that this Policy will be instrumental in the attainment of our long-term goal of Transformative legal education and critical input in the realization of our vision and mission.

On behalf of the Council, I commit our unwavering support to the implementation of this policy by assigning responsibility for implementation, oversight, and approving the necessary resources for implementation.

Prof. Collins Odote
Chairperson
COUNCIL OF LEGAL EDUCATION

ACKNOWLEDGMENT

This ICT Policy was developed through an elaborate consultative process that involved many stakeholders. It is aligned to the National Information, Communications, and Technology (ICT) Policy (2019) to realize the CLE's ICT potential in service provision to the stakeholders.

I wish to acknowledge the Council under the chairmanship of Prof. Collins Odote for their overall leadership of the process and for ensuring the Policy is approved to support the delivery of CLE mandate.

I appreciate the technical committee drawn from various Directorates and Divisions for the hard work, commitment and zeal in developing this Policy and Guidelines. It is also worth appreciating the role played by the ICT Division for providing excellent coordination, administration, and logistical support throughout the entire process. Many thanks also to the members of staff and stakeholders for providing invaluable contributions to better this policy.

Finally, I call upon CLE staff and stakeholders to support the implementation of this policy and guidelines to ensure the CLE reps the intended benefits.

Ms. Jennifer Gitiri, HSC
Ag. SECRETARY/CEO
COUNCIL OF LEGAL EDUCATION

POLICY APPROVAL

This Information and Communications Technology (ICT) Policy was duly adopted and approved by the Council in its meeting held on

the ...14th..... day of ......October...... 2024.

This Policy shall be reviewed as and when necessary. All amendments will be communicated in writing using the amendment sheet below. This will ensure that the ICT Policy remain consistent with the CLE's mandate and strategic direction.

Chairperson
COUNCIL OF LEGAL EDUCATION

Ag. Secretary/Chief Executive Officer
COUNCIL OF LEGAL EDUCATION

POLICY AMENDMENT SHEET

Issue/Revision No	Subject of Amendments	Reviewed By (Signature)	Review Authorized By (Signature)	Date

ABBREVIATIONS AND ACRONYMS

BCP	Business Continuity Planning
BYOD	Bring Your Own Device
CCTV	Closed-Circuit Television
CLE	Council of Legal Education
COBIT	Control Objectives for Information Technologies
FOSS	Free and Open Source Software
GoK	Government of Kenya
ICT	Information and Communication Technology
IS	Information System
ISMS	Information Security Management System
LAN	Local Area Network
MAC Address	Media Access Control address
PBMOK	Project Management Body of Knowledge
PPDA	Public Procurement and Asset Disposal Act
PRINCE 2	Projects IN Controlled Environments
SLA	Service Level Agreement
SCMD	Supply Chain Management Division
URL	Uniform Resource Locator
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity

DEFINITION OF TERMS

Asset Refers to a resource controlled by CLE and from which future economic benefits are expected to flow to the entity

Change The addition, modification, or removal of an IT service or service component and its associated documentation.

Cloud computing This is a model of computing where all the servers, networks, applications, and other elements related to data centers are made available to ICT and end users via the Internet, in a way that allows ICT service providers to buy only the type and amount of computing services that they need.

Commercial off-the-shelf software This refers to ready-made software installed at CLE.

Data Information that has been translated into a form that is convenient to transmit or process.

Database software is used to manage data.

Data Centre An ICT facility where equipment including servers, network equipment, and storage facilities are installed and operated to ensure they are protected from physical damage or tampering to ensure service availability.

Denial of service Procedures or actions that can prevent a system from servicing normal and legitimate requests as expected.

Hardware All CLE-owned computers and peripheral equipment (such as printers, scanners, network cards and multimedia equipment). Excluded from such equipment would be equipment that is already under an existing service contract, warranty, and non-standard ICT equipment for which only advisory information shall be provided.

ICT Refers to technologies that provide access to information through telecommunications. It primarily focuses on communication technologies. This includes the Internet, wireless networks, and other communication media.

ICT equipment Refers to any device that can process, store, or communicate electronic information, including computers, multifunction devices, landline and mobile phones, digital cameras, electronic storage media, and other radio devices.

DEFINITION OF TERMS

In-house development The software is developed using CLE's internal staffs.

Information System (IS) An Information system is a system that manages data needed by a business. It keeps records and maintains the various facts and figures needed to run the business. More specifically, an information system should support the day-to-day operations, management and decision-making information needs of business workers.

Patch A quick-repair job for a piece of programming designed to resolve functionality issues, improve security or add new features

Patch management The process of applying firmware and software updates to improve functionality, close security vulnerabilities and optimize performance.

Policy Principles or rules to guide decisions and achieve rational outcomes. A policy is a statement of intent and is implemented as a procedure or protocol.

Ping attack A form of a denial-of-service attack, where a system on a network gets "pinged," that is, receives an echo-request, by another system at a fast-repeating rate thus tying up the computer so no one else can contact it.

Software A program that allows access to computer hardware for purposes of processing data. System and software may be used interchangeably.

Request for Change (RFC) This is the formal change request, including a description of the change, components affected, business need, cost estimates, risk assessment, resource requirements, and approval status.

Vulnerability management A proactive strategy to identify, track, prioritize, and remediate security weaknesses and flaws in IT systems and software.

1. INTRODUCTION

1.2 Background

The Council of Legal Education is a corporate body established under the Legal Education Act, Cap 16B of the Laws of Kenya. CLE is mandated to regulate, supervise and license legal education programmes and legal education providers in Kenya. In addition, it administers the Advocates Training Programme (ATP) examination for purposes of admission to the Roll of Advocates in Kenya and advises the Government on matters germane to legal education and training.

CLE has been in existence since 2014 when it formally separated from the Kenya School of Law. CLE owes its existence to the recommendations of the Task Force on the Development of a Policy Framework for Legal Education and Training in Kenya, popularly known as the Muigai Taskforce which was appointed in 2004 with a fairly expansive mandate. One of its recommendations was to delink Council of Legal Education from the Kenya School of Law.

The recommendation was actualized by the enactment of the Legal Education Act No. 27 of 2012 and the Kenya School of Law Act No. 26 of 2012.The Legal Education Act became operational on 15th January 2013 ushering a new dawn for CLE.

1.2 Vision, Mission and Core Values

Vision

To Innovate Legal Professionals Transforming Society.

Mission

To ensure quality legal education through responsive regulation and administration of Bar Examination.

Core Values

i. Accountability

ii. Excellence

iii. Integrity

iv. Inclusiveness

v. Innovation

1.3 CLE Mandate

The mandate of CLE is outlined in the Legal Education Act CAP 16B as follows: -

i. regulate legal education and training in Kenya offered by legal education providers;

ii. license legal education providers;

iii. supervise legal education providers;

iv. advise the Government on matters relating to legal education and training;

v. recognise and approve qualifications obtained outside Kenya for purposes of admission to the Roll; and

vi. administer Advocates Training Programme examination.

1.4 Rationale

ICT plays a critical role at CLE in service delivery. CLE has invested heavily in ICT through systems anchored on its business processes. In order to protect the investment and ensure value realization the management has made a deliberate decision to formulate and implement this ICT policy. The following are the justification for this policy;

i) To safeguard the confidentiality, integrity and availability of CLE information systems;

ii) To provide guide CLE in embracing emerging technological advancements;

iii) To guide on automation of internal processes;

iv) To enhance the automation of services to the public;

v) To provide a framework for adopting Data Protection Act, 2019 (Cap 411C) and other relevant laws and regulations.

1.5 The Policy Objectives

i) To define what constitutes acceptable use of the ICT resources of CLE.

ii) To provide a guideline for the management of all ICT resources from procurement to disposal.

iii) To provide guidelines that ensure the availability, confidentiality, security, and integrity of CLE's information systems and its assets from any threats -

internal or external, deliberate or accidental.

iv) To provide guidelines on the use of e-mail services provided by CLE.

v) To provide a guideline on the user access management controls for CLE's ICT systems users both internal and external.

vi) To provide a standard guideline for the creation of strong passwords, protecting those passwords, and the frequency of change.

vii) To define an appropriate guideline for the use of the Internet by CLE's staff and affiliates.

viii) To outline guidelines that guide when planning for, organizing, and conducting ICT training at CLE.

ix) To provide a structured approach for responding to incidents that threaten ICT investments

1.6 Scope

i) This policy applies to all CLE and any other person(s) or organization(s) accessing services over CLE ICT resources; persons contracted to develop, repair, or maintain CLE's ICT resources and suppliers of outsourced ICT services.

ii) The ICT Policy defines and guides CLE's use of ICT resources, software, systems, hardware devices, infrastructure, network systems, and any other ICT solutions. The Policy shall also apply to all equipment owned or leased by CLE.

1.7 Normative Standards

The policies have been developed to be consistent with industry standards and is informed by the following industry standards:

i) Information Technology Infrastructure Library (ITIL)

The policy is aligned to the framework defined by the Information Technology Infrastructure Library (ITIL).

ii) Control Objectives for Information and Related Technology (COBIT)

The Policy conforms to Control Objectives for Information and Related Technology (COBIT 5) defines IT Governance framework and standards.

1.8 Legal and Regulatory Framework

This Policy is anchored on the following laws, rules, regulations, standards, and circulars:

i) The Constitution of Kenya, 2010.

ii) The National ICT policy, 2019.

iii) Access to Information Act, 2016 (Cap 7M), that provides the detailed framework on access to information held by the state.

iv) The Computer Misuse and Cybercrime Act, 2018 (Cap 79C), that provides a framework for handling ICT related offences.

v) The Data Protection Act, 2019 (Cap 411C), that defines the rights and protection of personal data.

vi) Kenya Information and Communications Act,2011 (Cap. 411A).

vii) CLE ISO Quality Systems Procedure.

viii) CLE HR policies and procedures.

ix) GoK ICT Standards

x) Public Service Code of conduct

2.HARDWARE, SOFTWARE, AND ACCESSORIES UTILIZATION AND MANAGEMENT

2.1 ICT Governance Policy

ICT governance is the process that ensures effective and efficient use of ICT in enabling CLE to achieve its goals. ICT Governance covers the culture, organization, policies and practices that provide oversight and transparency of ICT. The benefits of good ICT 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.

2.1.1 Purpose

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

2.1.2 Scope

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

i.) Alignment that provides strategic direction of ICT business processes

ii.) Value Delivery to ensure ICT services attain maximum value

iii.) Risk Management to ascertain that ICT business processes are in place and risks are managed

iv.) Resource management to give strategic direction for sourcing and use of ICT resources

v.) Performance to ascertain compliance and achievement of ICT objectives

2.1.3 Policy Statement

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

2.1.4 Policy Guidelines

i) CLE shall establish an ICT Steering Committee (ICTSC) in line with the ICT governance standard to provide oversight matters to issues related to ICT. ICTSC shall be responsible to the CEO and its broad functions shall include: -

  a) Monitor the progress of all activities arising from the implementation of CLE's ICT Policy.

  b) Develop and implement a workable ICT strategy for CLE.

c) Advise on a workable budget to manage and improve ICT resources and services for CLE.

d) Safeguard and make periodic reviews of ICT policies and regulations.

ii) CLE shall ensure that there is adequate staffing to manage ICT services and projects.

iii) CLE shall develop and implement, disseminate ICT service charter for all ICT enabled services.

iv) CLE shall allocate adequate funds to support ICT services through the annual budget.

v) CLE shall conduct and document customer satisfaction surveys on ICT enabled services annually for internal and external customers.

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

vii) CLE shall develop and implement annual preventive maintenance plans for ICT equipment.

viii) CLE shall ensure that ICT projects are conducted as per the GOK ICT project management standards.

ix) CLE shall acquire and install ICT help desk management system to handle all support requests from end users.

2.1.5 Enforcement

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

2.2 Acceptable Use of ICT Resources

2.2.1 Purpose

To ensure effective, efficient, and appropriate use of ICT resources by every user in CLE.

2.2.2 Scope

The scope of this policy applies to all CLE staff and Stakeholders accessing and utilizing CLE ICT resources and specifies authorized and unauthorized use. The ICT resources can either be owned or leased by CLE and will include the following: -

I) All ICT-related equipment, including personal computers, terminals, workstations, PDAs, projectors, scanners, cameras, CCTV, wireless computing devices, telecommunication equipment, networks, printers, servers, IoT and shared network resources, access controls, specialized equipment, and all peripherals.

ii) All electronic communications equipment, including telephones, mobile phones, hand-held devices, IP phones, wired or wireless communications devices and services, internet, intranet, e-mail, and other online services.

iii) All software including off-the-shelf, licensed business software applications, in-house developed applications, vendor/supplier customized applications, operating systems, databases, firmware, and any other software.

iv) All intellectual property and other data stored in CLE equipment.

2.2.3 Policy Guidelines

i) CLE ICT resources shall be used for authorized activities only.

ii) All staff shall ensure the efficient and appropriate use of ICT resources that guarantee the protection of individual rights.

iii) User directorate/ division shall have the responsibility to ensure that CLE systems developed and/or procured is used optimally. The ICT division shall be responsible for the back end of the system and ensure the system is available and secure for use.

iv) The ICT computing infrastructure and CLE systems shall be upgraded to newer versions from time to time and after a comprehensive review/assessment has been conducted. Recommendations made towards improvement of the same and in line with the relevant policies which may include feedback from CLE Stakeholders. Obsolete ICT assets may be disposed of as per CLE's Assets disposal policy.

v) All work produced using CLE ICT resources shall belong to CLE.

vi) Staff shall not use ICT resources improperly or infringe any legal rights.

vii) The use of CLE ICT resources by non-staff must be recommended by the Director/HoD of the user Directorate/Division and approved by the Head of ICT.

viii) ICT resources designated to divisions/directorates shall be moved after obtaining written authorisation from the respective Head of Directorates/Divisions.

ix) Any ICT resources shall be issued to users in consultation with the Director/HoDof the user Directorate/Division after a recommendation from the Head of ICT.

x) Technical requirements of systems developed/procured by CLE shall be developed by the ICT division in liaison with the user Directorate/ Division.

xi) The user Directorate/ Division shall ensure optimal utilization of all developed/ procured/customized modules and ensure the digitized processes are updated regularly.

xii) The ICT division shall ensure that ICT computing infrastructure and CLE systems are well maintained and upgraded when necessary.

2.2.4 Enforcement

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

2.3 Hardware Management Policy

2.3.1 Purpose

To protect and maintain ICT hardware in CLE to derive maximum value for the intended use and enhance efficiency and effectiveness in work performance.

2.3.2 Scope

This policy shall apply to all hardware in CLE. The hardware includes: Computers, Printers, Servers, Scanners, Projectors, photocopiers, UPS, network switches, access control, CCTV, Digital Cameras among others.

2.3.3 Policy Guidelines

The ICT division shall facilitate the acquisition, installation, configuration, testing, training and maintenance of equipment. As follows:

a) New ICT Hardware

i) Users shall sign for ICT hardware issued to them.

ii) ICT hardware shall be issued to all levels of staff based on the user requirements.

b) Hardware Replacement and Disposal

i.) Directorate/Divisions heads shall forward their requirements to the Head of ICT for planning and consideration.

ii.) The ICT Division shall verify and recommend the need for user hardware replacement or disposal.

c) Returning ICT Hardware

i) Returned hardware shall be subjected to quality checks before being accepted.

ii) Users shall sign a clearance form upon returning any issued ICT Hardware.

d) ICT Hardware Movement

i) Any ICT equipment leaving any CLE facility either for repair or being carried away by shall be issued with a gate-pass.

ii) ICT Division shall maintain an Internal hardware movement register with clear descriptions of the status/condition of hardware moved.

2.3.4 Enforcement

The management through the head of ICT division shall ensure compliance to this policy. Regular audits shall be carried out to ensure that assets are not being irregularly moved or transferred. Staff have a responsibility to ensure that they comply with this policy.

2.4 ICT Assets Management Policy

2.4.1 Purpose

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

2.4.2 Scope

This covers all CLE ICT assets and related equipment.

2.4.3 Policy Guidelines

i) CLE shall implement and maintain accurate, up to date, and consistent inventory of ICT assets.

ii) CLE shall undertake periodic review, access restrictions and classifications to sensitive assets, considering applicable access control policies.

iii) All ICT assets shall be assigned to individual user or to a Directorate / Division who shall be always held responsible for their care and security.

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

v) All staff and external party users shall return/surrender all of CLE ICT assets in their possession upon separation from CLE. Where a user has knowledge that is important to ongoing operations, that information shall be documented and transferred to CLE.

vi) Revaluation of all ICT assets shall comply with the provision of clause 7.5.2 of the Finance Policy and Procedure Manual 2023.

vii) ICT Division shall authorize movement, re-assignment or return assigned ICT asset except ICT assigned to Officers.

viii) In the event a CLE ICT asset is lost, the custodian shall notify the Head of ICT in writing immediately and report to the nearest Police station.

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

x) ICT Assets shall be disposed in compliance with the provision of CLE's Procurement and Asset Disposal Policy.

2.4.4 Enforcement

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

2.5 Acquisition of ICT Resources Policy

2.5.1 Purpose

To provide guidelines on the acquisition and ownership of ICT resources.

2.5.2 Scope

This Policy applies to all ICT resources acquired through procurement or under MOUs/grants/donations/agreements/gifts and the resulting ownership is transferred to CLE.

2.5.3 Policy Guidelines

i) All ICT resources acquired by CLE shall remain the property of CLE.

ii) All ICT resources acquired by CLE under Grants/ MOU/ Agreements or Donations shall have elaborate terms and conditions that include and specify ownership.

iii) The ICT Division, in collaboration with the user Directorate/Division shall develop technical specifications for the acquisition of ICT resources.

iv) All ICT resources acquired shall be managed by the ICT Division to ensure conformity to corporate standards.

v) All requisitions for procurement of hardware, software and specialized equipment shall be channeled through the head of ICT.

vi) Technical specifications shall be developed by the user Directorate/ Division in liaison with the ICT Division.

vii) ICT Division shall be involved in the procurement process of ICT resources that includes technical specifications development, evaluation, inspection, and acceptance/rejection.

viii) The ICT division shall ensure all ICT resources are installed, configured, tested, and commissioned as per the requirements.

ix) The ICT Division and SCMD shall ensure that all ICT equipment procured or granted to CLE shall be identified as belonging to CLE. The Division shall facilitate tagging or engraving of the asset for identification purposes.

x) Finance and Accounts Division shall capture the asset details in the asset inventory and copy maintained by the ICT, SCMD and HR Divisions.

xi) The ICT Division shall maintain an ICT Equipment register to log the movement of equipment to and from the Division.

xii) The ICT Division shall maintain an Inventory of machines that are out of warranty.

xiii) All procured ICT software, services, equipment, and items shall have warranties and user manuals.

xiv) The ICT Division shall standardize hardware configurations for computing devices that are supported by the Division.

xv) Installation, configuration, commissioning and training of procured ICT resources shall be done by the supplier/consultant/ contractor in liaison with the ICT Division.

xvi) The ICT Division shall manage all administrator accounts in computing devices, while members of staff shall operate from user accounts.

2.5.4 Enforcement

The management through the head of ICT division shall ensure compliance to this policy. Regular audits shall be carried out to ensure that they comply with this policy.

2.6 Repair and Maintenance Policy

2.6.1 Purpose

To provide guidance on systematic inspection, upgrade, downgrade, detection, reconfiguring, modifying, replacing or changing and servicing CLE ICT infrastructure. Maintenance shall include but not limited to software changes, hardware changes, network changes, patches and cabling.

2.6.2 Scope

The policy shall cover all CLE ICT computing infrastructure and accessories.

2.6.3 Policy Statement

CLE shall ensure that preventive, corrective, and adaptive maintenance for ICT infrastructure is undertaken regularly. CLE shall ensure that the maintenance contracts and preventive plans are reviewed periodically to ensure that they meet the required standards.

2.6.4 Policy Guidelines

i) Breakdown and/or malfunction of the ICT computing infrastructure shall be reported to Head ICT Division through Directorates/Divisions heads.

ii) Repair and maintenance of ICT computing infrastructure shall be coordinated by the Head of ICT Division. Where repair and maintenance is to be performed by an external entity, the Head of ICT division shall advise accordingly.

iii) The ICT division shall maintain proper documentation and inventory of repair and maintenance.

iv) The ICT, SCM and Legal Divisions shall prepare and maintain documentation and contracts of ICT computing infrastructure.

v) The ICT Division shall test the ICT computing infrastructure repaired and/or maintained. The inspection and acceptance committee shall prepare an acceptance/rejection report.

vi) Written notice of all scheduled maintenance of a significant nature shall be provided to staff and/or Public stating the nature of changes, and system impact as well as documenting the static time and duration of the maintenance.

2.6.5 Enforcement

Regular audits shall be carried out to ensure that they comply with this policy.

2.7 Software and Licensing Policy

2.7.1 Purpose

The purpose of this policy is to communicate to CLE staff the requirement regarding the use of computing software to facilitate efficient usage of resources.

2.7.2 Scope

This policy covers all software owned or installed in CLE ICT computing devices.

2.7.3 Policy Statement

All software is the property of CLE and shall be used by authorized CLE staff in furthering its mandate.

2.7.4 Policy Guidelines

i) All ICT equipment acquired and used in CLE shall run on genuine and licensed software.

ii) All software acquired for or developed on behalf of CLE shall be the property of CLE.

iii) All software licenses shall be managed centrally by the ICT Division through Active Directory Environment.

iv) Source code for all application software developed for CLE shall be the property of CLE.

v) Users shall request software through the Head of ICT.

vi) The head of ICT shall maintain records of software licenses owned by CLE.

Release of Software

i) CLE's Software shall not be loaned, traded, sold, given away, or otherwise divulged.

ii) Any upgrading, downgrading and updating of software shall be done by the ICT Division.

Custody of the software

i.) The ICT division shall have custody of all software owned or developed by CLE.

ii.) The ICT Division shall facilitate training for software use where necessary.

Acquisition and renewal of Licenses

The ICT division shall negotiate for the acquisition and renewals of licenses on behalf of CLE in liaison with the user and SCMD. The licenses

i) CLE shall comply with all laws regarding intellectual property. This applies to all Software licensed or developed in CLE.

ii) CLE may negotiate for corporate licenses.

iii) All purchased/customized software must be accompanied by the required licenses as per specifications.

iv) All acquired/customized/revised software shall be delivered with documentation.

Source Code

For developed software's, the source codes shall belong to CLE.

2.7.5 Enforcement

Regular audits shall be carried out to ensure that they comply with this policy.

2.8 Bring Your Own Device (BYOD) Policy

2.8.1 Purpose

CLE promotes use of user devices in the environment for access to information. The policy aims to manage user access, privacy, permission, loss and damage. The purpose of this policy is to provide guidelines to CLE staff on use of personally owned electronic devices within CLE premises.

2.8.2 Scope

This policy is applicable to anyone using a non-CLE 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 CLE.

2.8.3 Policy statement

The policy provides Council, staff and stakeholders with rules and guidelines on use of personal devices.

2.8.4 Policy Guidelines

i) 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.

ii) To prevent loss of CLE data, staff using their devices shall be required to use CLE cloud environment.

iii) The ICT Division will support the connection to CLE systems and accounts only where necessary. Users have a responsibility to learn how to use and manage their device effectively.

iv) CLE takes no responsibility for supporting, maintaining, repairing, insuring or otherwise funding staff user BYOD, or for any loss or damage resulting from support and advice provided.

v) Faults caused by user downloaded applications will not be rectified by ICT Division. Any application that causes security vulnerabilities will be denied access to CLE systems/networks.

vi) CLE shall provide guidance on software and malware issues, on a reasonable endeavor basis.

vii) CLE shall not take responsibility to implement the remedial actions.

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

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

x) CLE 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, candidates, business, reputation, systems or infrastructure.

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

xii) Any BYOD found to have the manufacturer's security mechanisms circumvented, such as 'jailbreak' will not be supported. CLE has the right to deny access to reduce the risk to its network.

xiii) BYOD shall only be allowed to CLE's network once proof of surety that the connection of the said device will not lead to denial or degradation of service to other users.

2.8.5 Enforcement

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

2.9 Disposal Policy

2.9.1 Purpose

To provide Policy guidelines for disposing unserviceable, obsolete, obsolescence, and surplus ICT equipment.

2.9.2 Scope

This Policy covers ICT equipment owned or operated by CLE.

2.9.3 Policy Statement

CLE shall ensure periodic assessment of ICT computing infrastructure to identify the equipment that cannot be reused or serviced. The identified unserviceable, obsolete, obsolescence, and surplus ICT equipment shall be disposed of in strict adherence to the Public Procurement and Asset Disposal Act, 2015 (Cap. 412C).

2.9.4 Policy Guidelines

I) The user Directorate/Division shall identify the ICT equipment that cannot be reused, serviced, or obsolete and forward them to the ICT Division for assessment.

ii) ICT equipment to be disposed of must be certified by Head of ICT. Equipment that has been certified unserviceable, or obsolete by ICT Division shall be forwarded to the SCMD for disposal.

iii) The process of evaluation of ICT hardware to determine whether it is more economical to repair, upgrade or replace ICT hardware components shall be done annually (the month of June) or upon approval by the Head of ICT to dispose obsolete equipment.

iv) ICT hardware shall be considered obsolete if the estimated cost of repair exceeds one-half of the current estimated value or they are damaged beyond repair.

v) ICT hardware and their accessories shall be considered uneconomical to maintain if the total cost of running them exceeds 60% of the cost of replacement and compatible replacements are not readily available.

vi) ICT equipment shall only be disposed of after making sure that all the data or information is backed up and permanently erased where applicable.

vii) CLE shall adhere to the Government guidelines when disposing of ICT storage media.

viii) Disposal of ICT equipment shall be undertaken by the Supplies Chain Management division according to the Public Procurement and Asset Disposal Act, 2015 (Cap. 412C).

ix) ICT equipment have a lifespan of four (4) years after which the process of disposal shall be initiated.

x) ICT equipment that are considered personal i.e. Mobile phones and tablets shall be retained by the user/custodian assigned when exiting CLE. (Valued and the officer given priority to purchase)

xi) All disposed ICT computing infrastructure shall be recorded, and the asset inventory updated accordingly.

2.9.5 Enforcement

Regular audits shall be carried out to ensure that they comply with this policy.

3. ICT SECURITY

3.1 Cyber Security Policy

3.1.1 Purpose

The purpose of this Policy is to establish guidelines on CLE cyber security risk management. The policy assigns responsibilities to all users based on the principle that cyber security is every user's responsibility. This underscores CLE's commitment to managing risks associated with ICT assets and information systems.

Cyber security controls shall be designed to facilitate individual users' cyber security awareness to enable accountability and trust; uphold confidentiality, integrity and availability of information assets; and allow for proactive plans and actions to detect, prevent and respond to cyber security threats; and support compliance with CLE's legal obligations, including in relation to data protection and privacy and security of critical infrastructure.

3.1.2 Scope

This policy shall apply to all users of CLE ICT infrastructure.

3.1.3 Policy Statement

CLE shall establish a cyber security policy for effective management of cyber security risks and protection from cyber threats that try to take advantage of opportunities in technology, people, and processes to harm or misuse CLE ICT infrastructure. Use of ICT Facilities and Services shall comply with CLE policies and relevant legislation.

3.1.4 Policy Guidelines

i) CLE shall develop and maintain Disaster recovery plans for security-critical applications and foundational ICT infrastructure.

ii) The associated monitoring and testing programs shall be approved annually to ensure effectiveness of cyber security that includes activities such as auditing, log and event analysis, vulnerability scanning, and penetration testing.

iii) A cyber security strategy and risk management responsibilities shall support the CLE Enterprise Risk Management Policy and utilize risk-based decision-making to manage cyber security risks.

iv) The ICT facilities and Services shall be provided, managed, and operated such that: The 'Critical Security Controls' maintained by the Centre for

Internet Security are adopted to establish a broad and effective defensive base.

v) Security critical infrastructure, application services and data shall be individually identified and subjected to risk-based management and additional controls as appropriate.

vi) The responsibilities of various players shall be;

a. **The Secretary/ CEO**

i) Appoint a Cyber Security team;

ii) Authorize complementary operational procedures to support this policy.

iii) Authorize the isolation or disconnection of any equipment or ICT facility from CLE network which poses a severe and unacceptable risk.

b. **The Head of the ICT Division**

i) Responsible for coordinating the implementation of Cyber Security Policy and supporting framework;

ii) Undertaking routine monitoring programs to ensure the effectiveness of Cyber security measures;

iii) Undertaking testing programs to ensure the effectiveness of disaster recovery plans;

iv) Preparing and submitting reports on cyber security to Management and the relevant Committee of the Council.

v) Conduct education activities to ensure awareness of cyber security threats and defenses.

c. **Relevant Council Committee**

i.) Oversee the adequacy of cyber security capability and controls.

ii.) Receive and review reports on cyber security risks and controls;

d. **Staff with Responsibility for Managing ICT Facilities**

I) Operate and manage the ICT facilities according to CLE Cyber Security policies and procedures;

ii) Regularly monitor and assess the related cyber security controls to ensure effectiveness; and

iii) Immediately report all security incidents and breaches to the head of ICT.

e. Users of CLE ICT Facilities and Services

i.) Adhere to ICT cyber security policy while using CLE facilities and Services at all times;

ii.) Be aware of security requirements of the ICT Facilities and Services they use, and take every precaution to safeguard their access to these systems against unauthorized use; and

iii.) Immediately report any known or suspected security incidents and breaches to the head of ICT.

3.1.5 Enforcement

Regular audits shall be carried out to ensure that they comply with this policy.

3.2 Password Security Policy

3.2.1 Purpose

Passwords shall be the entry point to all ICT resources. Protecting access to resources is pivotal in ensuring that systems remain confidential, available and with integrity. The purpose of this policy is to establish a standard for creation, protection, use and change of passwords.

3.2.2 Scope

The scope of this policy covers any person with an account on any CLE information system within CLE network and has access to CLE network or stores any CLE information.

3.2.3 Policy Statement

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

3.2.4 Policy Guidelines

i) Password construction requirements shall satisfy the following criteria on all CLE systems:

i. Shall be a minimum length of eight (8) characters: uppercase—for example, A to Z, lowercase—for example, a to z, numeric—0 to 9, non-alphanumeric—symbols such as! #, %, or &

ii. Shall not be a dictionary word or proper or common name.

iii. Shall not be the same as the user ID.

iv. Shall expire within a maximum of Sixty Days (60) calendar days.

v. Shall not be identical to the three (3) immediate previous passwords.

vi. Shall not be transmitted in clear or plaintext outside the secure location.

vii. Shall not be displayed when entered.

viii. Shall only be reset for authorized users.

ix. The account user shall be notified of all password changes

x. Two factor authorization shall be implemented for password change.

ii) Passwords shall be kept confidential

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

iv) Passwords shall not be transferred or shared with others.

v) If an account or password is suspected to have been compromised, the incident shall be reported to the head of ICT immediately.

vi) Prompts to change passwords after first log in using default password. Default passwords shall be changed immediately on all equipment after the first login.

vii) Enable self-change of password

Disabling an Account

All accounts that are no longer in use shall be disabled immediately. These include, but is not limited to, the following:

i) Separation of staff.

ii) Contractor accounts, when no longer needed in performance of any duties.

Standards for application development

Application developers shall ensure their programs contain the following security precautions:

i) Support authentication of individual users, not groups.

ii) Passwords are not in clear text or any easily reversible form.

iii) Provide role management so that one user can take over the function of another without having to know the other's password.

3.2.5 Enforcement

Regular audits shall be carried out to ensure that they comply with this policy.

3.3 Antivirus Management Policy

3.3.1 Purpose

To protect CLE's ICT resources from attacks by malicious software such as computer viruses, worms, Trojan horses, spyware, root kits and botnet. Defenses against computer viruses include protection against unauthorized to computer systems, using only trusted sources for data and programmes, and maintaining virus-scanning software.

3.3.2 Scope

This policy applies to all ICT resources and staff of CLE in regards to cyber security.

3.3.3 Policy Statement

CLE shall apply a dual anti-virus policy such that where there is connectivity, it will install a corporate antivirus and areas where there is no connectivity, single user antivirus shall be installed.

3.3.4 Policy Guidelines

The following guidelines are to assist in the prevention of virus attacks: The ICT Division shall:

i) Install and maintain appropriate licensed antivirus software on all computing devices and shall be configured to perform daily full-system and on-access scans.

ii) Ensure regular updates and upgrades of the antivirus.

iii) Respond to all virus attacks, eliminate any virus detected and document each incident and inform the users of infected computers of the action taken immediately.

iv) Update regularly antivirus software on standalone devices.

v) Ensure that antivirus is always enabled.

All Users Shall:

i) Not introduce a computer virus into computing devices/network

ii) Not load removable storage of unknown origin into CLE computing devices or network

iii) Not download files/attachments from unknown or suspicious sources.

iv) Scan removable media for viruses before being accessed.

v) Immediately shut down the workstation and inform the ICT Division if they suspect that their workstation has been infected by a virus.

vi) Neither open nor forward attachments/files to an email from an unknown, suspicious or untrusted source. These attachments must be deleted immediately, and deleted again by emptying the recycle bin.

vii) Avoid direct disk sharing with read/write access unless absolutely necessary.

viii) Regularly update the antivirus software.

3.3.5 Enforcement

Regular audits shall be carried out to ensure that they comply with this policy.

3.4 Backup and Recovery Policy

3.4.1 Purpose

This policy is designed to protect data against loss and recover it in the event of an equipment failure, data loss, intentional or unintentional destruction of data, or disaster.

3.4.2 Scope

This policy applies to all core business data and systems, staff of CLE, and external service providers who may be responsible for the installation, support and security of data and information.

3.4.3 Policy Statement

All CLEs' systems data shall be backed up and securely stored on site and off site.

3.4.4 Policy Guidelines

The ICT Division shall ensure that backup and recovery procedures for each system are documented and periodically reviewed.

i.) Secure backups shall be taken on external media and may incorporate data encryption.

ii.) Backups shall be stored on site and off site securely.

iii.) A process shall be implemented to verify the success of the backups.

iv.) The head of ICT shall establish and formally document an appropriate schedule for full and incremental backups.

v.) Backups shall be periodically tested to ensure that they are recoverable.

vi.) Authorised staff access lists to offsite backup storage shall be reviewed periodically or when an authorised staff leaves CLE or Division.

vii.) A quarterly report shall be presented to the relevant Council committee, on authorised staff access lists to offsite backup storage.

viii.) The ICT Division shall be responsible for:

   i. Perform and verify backups for core systems,

   ii. Check that they have been successfully completed,

   iii. Record the information on the backup register,

   iv. Ensure that the backups are stored securely.

3.4.5 Enforcement

Regular audits shall be carried out to ensure that they comply with this policy.

3.5 CCTV Policy

3.5.1 Purpose

CLE uses closed circuit television (CCTV) images to protect its property and to provide a safe and secure environment for staff and visitors within CLE's premises. This policy sets out the details of how CLE will collect, use and store CCTV images. The planning and design of CCTV systems will endeavor to ensure maximum effectiveness and efficiency.

3.5.2 Scope

This policy applies to all CLE premises where the installation of CCTV has been implemented.

3.5.3 Policy Statement

CCTV systems have a legitimate role to play in helping to maintain a safe and secure environment for both staff and visitors. Images recorded by surveillance systems are personal data which must be processed in accordance with data protection laws. We are committed to complying with our legal obligations and ensuring that the legal rights of staff, relating to their personal data, are recognized and respected.

3.5.4 Policy Guidelines

The following guidelines are to help in monitoring of the CCTV systems:

i) ICT Division shall ensure that CCTV cameras are working at all times and are capturing footage constantly in real-time. The cameras should be strategically placed, and that the footage is accessible as and when required.

ii) Access to, and disclosure of, images recorded on CCTV shall be restricted. This ensures that the rights of individuals are retained.

iii) ICT Division shall facilitate the viewing and disclosure of CCTV footage. The request should be in writing and it shall include, the date of the disclosure, to whom the images have been provided and the reasons why they are required. If disclosure is denied, the reason will be recorded.

iv) The Accounting Officer shall authorize disclosure of footage to external third parties such as law enforcement agencies while the Head of ICT shall authorize internal requests for viewing of footage.

v) ICT Division shall ensure back-up of CCTV footage is maintained as per CLE's back-up processes and procedures manual.

vi) ICT Division shall ensure that the CCTV footage is retained/archived according to the Public Archives and Documentation and Services Act Cap 19 and in reference to the CLE archives & records management policy.

vii) At all times, the CCTV footage access and disclosure shall abide with the Data Protection Act, 2019 (Cap 411C), its Regulations and applicable laws that pertains to release of personal and sensitive data.

viii) The CCTV cameras shall be used to capture footage/ images of events/ occurrence within CLE premises.

ix) The recorded events/occurrences shall not be used for any commercial purposes.

x) The day-to-day functionality and monitoring of the CCTV system shall be the responsibility of the ICT Division.

xi) ICT Division shall be responsible in the management of the technical aspect of the CCTV system by ensuring uptime of the system.

xii) The footage produced by the CCTV equipment shall be as clear as possible so that it is effective for its intended purpose.

xiii) As the recording system records digital images, any CCTV images that are held on the hard drive of a PC or server are deleted and overwritten on a recycling basis and, in any event, once the hard drive has reached the end of its use, it will be erased prior to disposal.

3.5.5 Enforcement

Regular audits shall be carried out to ensure that they comply with this policy.

3.6 Access Control Policy

3.6.1 Purpose

The Access Control policy outlines the regulations, permissions, and limitations governing all users' access to CLE's assets, including logical and physical entry points.

3.6.2 Scope

This policy applies to all CLE's premises, staff and other stakeholders accessing CLE premises.

3.6.3 Policy Statement

CLE is dedicated to upholding robust access controls to protect information and systems from unauthorized access, identify staff and monitor attendance. CLE shall endeavor to preserve data confidentiality, integrity, and availability.

3.6.4 Policy Guidelines

i) CLE shall install a biometric system with access points located at entry/exit points.

ii) The ICT Division shall assign asset owners, ensure the least privileged access is implemented make configuration changes to the access control system.

iii) All staff/interns/attaches/temporary staff shall be required to be enrolled in the biometric/access card for the purpose of gaining access to CLE's premises.

iv) Staff shall clock in and clock out during official working days.

v) The ICT Division shall facilitate access to biometric data to authorized officers through the approval of the Accounting Officer.

xiv) The ICT Division shall ensure that the Access control logs is retained/archived for a period of 90 days in accordance with the Public Archives and Documentation and Services Act Cap 19 and in reference to the CLE archives & records management policy.

vi) The Human Resource and Administration Division shall communicate in writing to the ICT Division on officers to be deactivated from the biometric system.

vii) The Head of ICT shall be responsible for the management of the technical aspect of the biometric system by ensuring uptime.

Access to Data Centre

i) Physical access to the Data Centre area shall be controlled and only authorized persons shall access the same.

ii) All visiting delegations shall have prior appointments approved by the Accounting Officer and must be accompanied by an authorized officer within these restricted areas.

iii) All entries and exits of every visitor and third parties must be logged in a register which is always maintained at the Data Centre.

iv) Visitors are prohibited from taking photographs and videos within the data centre. -

v) Eating and drinking in the data centre is prohibited.

vi) The data centre shall be equipped with fire suppression and detection systems, fire extinguishers, air conditioning, backup power as per international best practices.

Data Centre Environment

i) Hand-held fire extinguishers shall be placed in strategic positions in the Data Centres. They shall be inspected annually.

ii) Smoke Detectors shall be placed above and below the ceiling tiles throughout the facility and below the raised Data Centre. They shall produce an audible alarm when activated.

iii) Fire suppression system shall be installed. The system shall not damage the equipment.

iv) Regular inspection by the contractors or suppliers shall ensure that all fire detection systems comply with building codes. The Human Resources and Administration Division shall facilitate inspection of the system annually.

v) The data Centre shall have an automatic emergency power-off switch, to shut off computers and peripherals in case of an emergency.

3.6.5 Enforcement

Regular audits shall be carried out to ensure that they comply with this policy.

3.7 Server Audit Policy

3.7.1 Purpose

Servers store critical information and are required to perform optimally throughout their life- cycle to provide quality service to users. Servers in CLE support critical business functions and store information. Improper configuration of servers can jeopardize the confidentiality, availability and integrity of data and application systems. The purpose of this policy is to ensure confidentiality, integrity and availability of information and resources.

3.7.2 Scope

This policy covers all servers owned or operated by CLE. This policy applies to ICT staff, system and server administrators, internal and external server auditors as well as all CLE staff.

3.7.3 Policy Statement

A general audit of the servers shall be undertaken regularly to provide an independent appraisal and recommend security improvement where necessary.

3.7.4 Policy Guidelines

i) All servers owned or operated by CLE shall be configured according to CLE security policies.

ii) Approved and standard configuration templates shall be used when deploying server systems.

iii) External auditors shall be allowed access to CLE servers to the extent necessary to allow them perform scheduled and ad hoc audits of all servers through the Accounting Officer's authority.

iv) ICT division shall conduct continuous self-assessment audits and advise the Accounting Officer accordingly.

v) Both Internal and external auditors shall never use access granted for any other purpose other than the server audit.

vi) CLE servers shall be audited at least annually according to the Government guidelines or on a need basis.

vii) The Head of ICT shall facilitate the Audit of CLE servers.

viii) All relevant findings discovered as a result of the audit shall be listed in CLE tracking system to ensure prompt resolution or appropriate mitigating controls.

ix) All results and findings generated by the audit team shall be provided to Management after completion. This report will be the property of CLE and shall be deemed confidential.

x) The ICT division shall ensure.

I. All system logs shall be contained in a secured central log review system.

II. All Administrator actions must be logged.

III. Use of a central patch deployment system.

IV. Host security agent such as antivirus is installed and updated.

V. Network scan to verify only required network ports and network shares are not interfered with.

VI. Verification of administrative group membership.

VII. Baselines assessment are conducted when systems are deployed and upon significant system changes.

VIII. Changes to configuration template is coordinated with approval of the ICT division.

3.7.5 Enforcement

The Head of the ICT division shall ensure adherence to the requirements of this policy.

4. NETWORK MANAGEMENT

4.1 Network Management Policy

4.1.1 Purpose

To centrally and strategically coordinate network infrastructure planning and implementation.

4.1.2 Scope

The policy covers all network infrastructures such as Local Area Networks, Wide Area Networks and Wireless Networks; active devices such as firewalls, switches, routers, DTUs; cabling, bandwidth, internet, access points, IP Phones, Landline and controllers.

4.1.3 Policy Statement

Network infrastructure shall be centrally planned, managed and maintained by the ICT Division.

i) All network infrastructures shall incorporate firewalls, VLANs, NAT, encryptions, VPNs, intrusion detection systems, intrusion prevention systems and Network Management System, Network Admission Control among others.

ii) VPN access is controlled using username and password authentication as is contained in CLE's active directory.

4.1.4 Policy Guidelines

i) All requests from user Directorates/Divisions for networks such as LAN, WAN and wireless connectivity shall be made to the ICT Head for appropriate advice and action.

ii) The ICT Division shall conduct a feasibility study before technical specifications and network layout designs are developed.

iii) The ICT Division shall protect the networks and systems for which they are responsible and monitor performance.

iv) The ICT Division shall carry out bi-annual vulnerability tests, review and implement recommendations of the report.

v) The ICT Division shall constantly monitor network activity as necessary for detection of unauthorised activity and security against threats, intrusion attempts, and compromised equipment among others.

vi) The ICT Division shall maintain network infrastructure designs, architectures, installations, configurations and documentation.

4.1.5 Enforcement

The Head of the ICT division shall ensure adherence to the requirements of this policy.

4.2 Email Policy

4.2.1 Purpose

Email service is a key communication tool in CLE. The purpose of this policy is to guide on appropriate use of the email service within CLE.

4.2.2 Scope

The scope of this policy covers the creation, use, and management of email services, and shall apply to Council, Staff, and stakeholders.

4.2.3 Policy statement

The Email services shall be located in the cloud and provide a convenient solution to store or share information over the Internet. The Council, Staff, and Stakeholders shall observe the guidelines outlined in this policy to ensure the proper use of the organization's electronic communication.

4.2.4 Policy Guidelines

i) Council, staff and other authorized personnel shall be facilitated with a CLE email account.

ii) The email address format shall have the initial of the first name, the full last name, and @cle.or.ke e.g. ksheria@cle.or.ke. Staff email accounts may belong to one or more email groups. Exceptions shall be given for staff with similar names to use full names.

iii) The users shall not block, mark as spam, blacklist other users within CLE domain.

iv) CLE email account shall only be used for CLE's purposes.

v) Use of email must be consistent with the ICT Acceptable Use policy, network security policy, other policies and procedures, and applicable laws.

vi) Correspondences sent, received, forwarded, or shared on CLE individual email or group emails shall be taken as duly and officially communicated.

vii) Sending, forwarding, or otherwise transferring inciting and offensive emails constitutes unacceptable use of the emails and is prohibited. Sending chain letters, press releases, joke emails, or other junk mail of any kind is prohibited

viii) CLE shall uphold the Kenyan Laws on Retention of Electronic Records as stipulated in the Kenya Information and Communications Act,2011 (Cap. 411A).

ix) CLE staff shall not, under any circumstances, use, monitor, intercept, or browse other users' e-mail addresses without authorization.

x) CLE reserves the right to inspect, copy, remove user data to investigate operational problems or for the detection and investigation of suspected misuse.

xi) CLE reserves the right to access and disclose the contents of a user's e-mail messages, by its legal and audit obligations, and for legitimate operational purposes.

xii) CLE reserves the right to demand that encryption keys, where used, be made available to fulfill its right of access to a user's e-mail messages in such circumstances under Clause x and xi.

xiii) CLE staff holding mail messages, e-mail addresses (or any other confidential material) shall be password protected.

xiv) Staff proceeding for leave are encouraged to use autoreply for out-of-office.

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

i. Consider using attachments to communicate lengthy emails.

ii. Write well-structured emails and use short, descriptive subjects and straight-to-the-point sentences.

iii. Signatures must include your name, job title, and name of the Directorate/Division

iv. The Council email disclaimer shall be added underneath your signature

v. Users must spell-check all emails prior to transmission.

vi. Email to be sent must be carefully composed, addressed and sent only to the intended recipients.

vii. Email to be sent must be appropriate, legal, legitimate and ethical under the context of this policy.

4.2.5 Enforcement

CLE shall ensure compliance with this policy, any violation may be subjected to disciplinary actions as per the Human Resource Policies and Procedure Manual, and other relevant laws and regulations.

4.3 Website Management Policy

4.3.1 Purpose

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

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

4.3.2 Scope

This policy governs web-based applications and documents made available via CLE domain cle.or.ke and its sub domains.

4.3.3 Policy Statement

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

4.3.4 Policy Guidelines

i) CLE 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 divisions

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

iii) CLE shall ensure websites are designed with consistent layout, usability, inter-operability.

iv) CLE 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.

v) CLE 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.

vi) CLE website shall not be used for commercial purposes that are not related to CLE mandate.

vii) CLE website shall be designed, managed and maintained in accordance to the GoK ICT standards.

4.3.5 Enforcement

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

4.4 Change Management Policy

4.4.1 Purpose

The purpose of this policy is to establish a framework for change management in ICT infrastructure and technologies. Change can disrupt service provision and therefore needs to be managed in a structured manner to ensure seamless transition.

4.4.2 Scope

This policy applies to all users, management and stakeholders who are involved or are affected by the changes.

4.4.3 Policy Statement

All changes shall follow the appropriate ICT change management policy to minimize adverse impacts to CLE operations and to users of CLE ICT services.

4.4.4 Policy Guidelines

i) All changes shall be initiated through a Request for Change (RFC) form by an authorized officer with the approval of the CEO. The RFC shall contain relevant information to enable evaluation of the benefits and the risks associated with the change. The procedures for change management appropriate to the classification shall be followed.

ii) Changes to the ERP shall be logged and an alert sent to the CEO in real-time.

iii) Users shall test the Change before its fully adopted to ensure that the change is working as expected.

iv) Users shall be trained on the new operational processes impacted by the change and sign off.

v) A customer satisfaction survey shall be carried out three months after implementation of the change.

vi) All change management procedures shall include the following activities:

a. Change Classification: Each change shall be classified according to the category of the change requested and timelines. This will be used to determine the procedures that are to be followed.

b. The evaluation will take into consideration the feasibility; human and physical resource requirements and costs; impact on the services provided to internal and external customers during the change; impact on services provided following the change; information security and risks.

c. The Head of ICT shall authorize the change based on the recommendation of the evaluation.

d. The change shall be scheduled at a time that will minimize disruption to operations.

e. Notification on the time, duration and services that could be affected shall be sent to all CLE stakeholders affected by the change.

f. The change shall be tested successfully in a test environment before it is implemented by an independent team.

g. A roll-back plan shall be developed and implemented before the change is carried out.

h. Users shall be notified on the results of the change once the change process is completed to satisfaction

4.4.5 Enforcement

The Head of the ICT division shall ensure adherence to the requirements of this policy.

4.5 Vulnerability and Patch Management Policy

4.5.1 Purpose

The purpose of this policy is to enforce Vulnerability and Patch Management for CLE - owned or managed ICT Resources.

4.5.2 Scope

This Policy applies to all systems operated or owned by CLE.

4.5.3 Policy Statement

The policy supports the Information Security Policy. It details requirements for maintaining up-to-date software version levels and operating system security patches on all ICT systems.

4.5.4 Policy Guidelines

Patch Management;

i) ICT systems shall be manufacturer-supported and have up-to-date and security-patched operating systems and application software.

ii) Security patches shall be installed to protect ICT assets from vulnerabilities.

iii) The head of ICT division shall ensure patches are tested before release for implementation.

iv) Patches rated 'Critical' by the vendor shall be installed within 3 days of release from the operating system or application vendor unless prevented by CLE change management policy.

v) Patches rated 'High' by the vendor shall be installed within 7 days of release from the operating system or application vendor unless prevented by CLE change management policy.

vi) Patches rated 'Low' or 'Medium' by the vendor shall be installed within 10 days of release from the vendor, unless mitigating controls are in place to prevent the exploit from being realized, in which case it may be deferred to the nearest maintenance window period.

vii) Users shall reboot their device/s when prompted to do so. Rebooting a device may be deferred to a maximum of two times (critical rated patches exempted) within the first 3 days of a patch being deployed by ICT Division, after which it shall be automatically rebooted.

viii) Patching of CLE systems shall be centrally managed wherever possible unless there are clear reasons for patching to be performed locally.

Vulnerability Management:

i) The ICT division shall conduct continuous vulnerability assessments of CLE systems. Targeted vulnerability assessments may also be implemented on need basis, determined and administered by the ICT Division or an authorized entity.

ii) Users shall allow access to approved CLE Vulnerability Management Agent or allow for the ability to run authenticated vulnerability scans.

iii) Use of any network-based tools to scan or verify vulnerabilities must be approved in advance by the CEO.

iv) Once vulnerability assessments have been conducted, the ICT division shall communicate to users. It is the responsibility of the users to support fully any vulnerability assessment being conducted on systems for which they are accountable.

v) CLE may engage with third parties to conduct internal or external vulnerability assessments or penetration testing as necessary through the CEO.

vi) The head of ICT division reserves the right to remove or isolate vulnerable assets from CLE's network at any time without prior communication. Once the cyber threat is contained, the ICT Team will work with the user to seek a resolution.

4.5.5 Enforcement

The Head of the ICT division shall ensure adherence to the requirements of this policy.

5. ICT SERVICE MANAGEMENT

5.1 User Support Policy

5.1.1 Purpose

This policy provides guidelines on services provided by the ICT Division at CLE with an aim of accelerating expeditious delivery of the mandate. These services include but not limited to internet provision, e- mail, hardware support, IP telephony, training, system and software development and support and advisory on emerging ICT Technologies.

5.1.2 Scope

This applies to all CLE staff.

5.1.3 Policy Statement

The ICT Division shall endeavour to provide quality support to all users as per the ICT Division user support procedures.

5.1.4 Policy Guidelines

i) ICT Division shall ensure that all ICT support requests shall be documented

ii) There shall be an ICT Service Charter that shall give guidelines on services provided by the ICT Division to ensure that CLE staff are empowered to achieve operational efficiency in the performance of their duties.

iii) Users shall immediately contact the ICT Division when they have ICT related issues.

iv) The ICT Division shall be committed to offer ICT related support as stipulated by ICT service charter and process and procedures manual.

v) The ICT Division shall review the ICT Service charter after every three years.

vi) To ensure that all documentation for ICT resources is well-kept for referencing and continuity purposes. The documentation includes among others:

a) Service Level Agreement

b) Contracts

c) Networks designs, architecture and configurations

d) Project documentation

e) Inspection and Acceptance reports

f) System audit reports

g) User requirements and technical specifications

h) User manual

i) Technical manual

j) Installation and recoverable disks

k) Feasibility study report

l) Systems design report

vii) It shall be the responsibility of the ICT Division and SCMD to have custody of the documents indicated above.

viii) It shall be the responsibility of all contractors where applicable to provide documentation as indicated in the scope:

ix) Documentation shall be stored both in hard or soft copy.

5.2 ICT Training Policy

5.2.1 Purpose

To build capacity for CLE staff members and stakeholders on ICT skills and competencies to ensure they are kept abreast with the emerging trends in ICT in line with HR policies and procedures.

5.2.2 Scope

This Policy shall apply to all CLE staff and stakeholders.

5.2.3 Policy Statement

CLE shall implement this training Policy to ensure that staff and stakeholders undergo continuous capacity building to keep abreast with emerging trends and technologies.

5.2.4 Policy Guidelines

i) The head of ICT shall compile Divisions' Training needs on an annual basis and forward them to HR to be included in CLE training Plan.

ii) CLE shall facilitate ICT officers to attend relevant seminars, and workshops to enhance their skills and gain exposure to new and emerging technologies.

iii) CLE shall ensure that all ICT projects, hardware, and software acquired have the necessary training components such as:

a) Technical user training

b) Management user training

c) Operational user training

d) Trainers of Trainers (TOTs)

iv) CLE shall ensure that staff are periodically sensitized on ICT to enhance their skills.

v) The head of ICT Division shall ensure staff are trained on ICT emerging technologies from time to time.

vi) The head of ICT Division shall ensure that systems user manuals are available for training and reference purposes.

vii) The head of ICT Division shall sensitize new users on CLE ICT infrastructure.

Cyber Security Awareness

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

i) CLE staff shall be provided with information security awareness tools to enhance their knowledge regarding the range of threats and appropriate safeguards that may result from sensitive data being acquired unlawfully, damaged, or modified.

ii) Third-parties and temporary personnel shall be briefed on CLE information security policies before being allowed to undertake any project within CLE to avoid data loss in error or through negligence.

iii) The head of ICT Division shall train all authorized systems users to ensure that their use is efficient and does not compromise information

5.3 Emerging Technologies and Innovation Policy

5.3.1 Purpose

Innovation has become crucial to an organization's growth, sustainability, efficiency and competitiveness. CLE recognizes the need to provide an enabling environment to foster innovations and enhance its 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 non-existence or obscurity. Innovation in organizations can be suppressed 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 CLE to achieve maximum benefits.

5.3.2 Scope

The policy covers all CLE ICT innovations and emerging technologies and shall apply to all CLE staff and its stakeholders.

5.3.3 Policy statement

CLE shall remain cognizant and duly consider emerging technologies to advance and improve its service delivery. CLE shall foster innovations to strengthen its capability to generate, transfer, and apply technologies; and ensure sustainable utilization of the organization's resources for the realization of CLE development objectives.

5.3.4 Policy Guidelines

i.) CLE staff are encouraged to develop ICT solutions to improve on service delivery.

ii.) CLE shall create a conducive environment to promote research and development as well as innovative initiatives within the organization.

iii.) ICT division shall conduct continuous research on emerging technologies with a view of incubating and adopting them for operationalization.

iv.) ICT division shall establish a knowledge base in CLE's resource center for ICT research and innovation.

v.) CLE shall protect its innovations and intellectual assets in line with the CLE Intellectual Property Policy.

vi.) CLE may commercialize innovation as a revenue generating activity.

5.3.5 Enforcement

CLE shall ensure compliance to this policy.

5.4 Electronic Records Management Policy

5.4.1 Purpose

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 CLE will include data or communication generated by CLE computer software and systems and stored in databases. The purpose of this policy is to effectively manage electronic records and improve both internal efficiency and overall organizational goals.

5.4.2 Scope

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

5.4.3 Policy Statement

CLE 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 CLE's primary systems used for the storage of digitized documents to ensure their authenticity and reliability.

5.4.4 Policy Guidelines

i) CLE shall deploy Electronic Record Management Systems to create, maintain, disseminate and administer electronic records

ii) The Electronic Record Management System 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.

iii) CLE shall digitize records for better management

iv) CLE shall protect e-records to enable their accurate and ready retrieval throughout their retention period

v) 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.

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

vii) CLE shall adopt and use of records retention and disposal schedules in compliance with the Kenya National Archives and Documentation Services Act Cap 19, Including the Records Disposal Act Cap 14 and in line with CLE Records & Archives Management Policy.

5.4.5 Enforcement

Quarterly checks will be carried out by ICT Division to ensure policy is being applied. These checks and any remedial action taken shall be recorded.

6. APPENDICES

6.1 Appendix I: Inventory Management Form

REPUBLIC OF KENYA

COUNCIL OF LEGAL EDUCATION

Inventory Management Form

User Information

Full Name:

First Name **Middle** **Last Name**

Staff No.: **E-mail Address**

Directorate: **Division:**

PC / Laptop Information

PC / Laptop Type

Server Computer.: □ Personal Computer PC: □ All-in-ones

Desktop: □ Laptop: □ Others: ....

PC / Laptop Manufacturer

HP.: □ DELL: □ Apple: □ Acer: □ ASUS □ Toshiba □ Lenovo □

Others: ....

PC / Laptop RAM

2 GB.: □ 8 GB: □ 32 GB: □ 128 GB: □

4 GB: □ 16 GB: □ 64 GB: □ Others: ....

Model: .... Location... Serial No: .... Screen Size................................ HDD: □ Size......... SSD: □ Size ....Processor.......................

Software / Network Information

PC / Laptop Operating System

Ubuntu. □ Windows 7 □ Windows 8 □ Windows 10 □ Windows 11 □

Others: ....

PC / Laptop Microsoft Office

Office 2003 □ Office 2007 □ Office 2016 □ Office 2019 □

Others: ....

Download Google Chrome □ Adobe Acrobat Reader: □

WinRAR: □ Others:
....
....

PC / Laptop Antivirus **IP Address**

Kaspersky endpoint security □ Static □ Dynamic □

Kaspersky Netagent □ IP Address: ....

MAC Address: ....

Accessories Information

Printer Manufacturer

HP.: □ DELL: □ Epson: □ Acer: □ ASUS □ Toshiba □ LEMOVO □

Others: ....**Printer Model:**
.... Serial No: .... UPS
Manufacturer...**UPS Rating:**
.... Serial No: ....

Other Accessories Comments

....
....
....
....
....

User Agreement and Certification

The use of the computer facilities is granted to the undersigned only. The undersigned shall not allow another person to use their username and password. CLE's computing resources are provided primarily for academic purposes, including education, research, communication, and college administration.

The undersigned agrees to abide by the guideline

Date: ______________________________ **Signature:** ______________________________

To be completed by the ICT Division

ICT Staff

Date: Signature:

ICT ASSET HANDOVER

PC / Laptop Manufacturer

HP.: □ DELL: □ Apple: □ Acer: □ ASUS □ Toshiba □ Lenovo □

Others: ……………………………………………………………………………

Model: ……………………………………. Serial No: ………………………..

Accesorries……………………………………………………………………………………………………

……

……

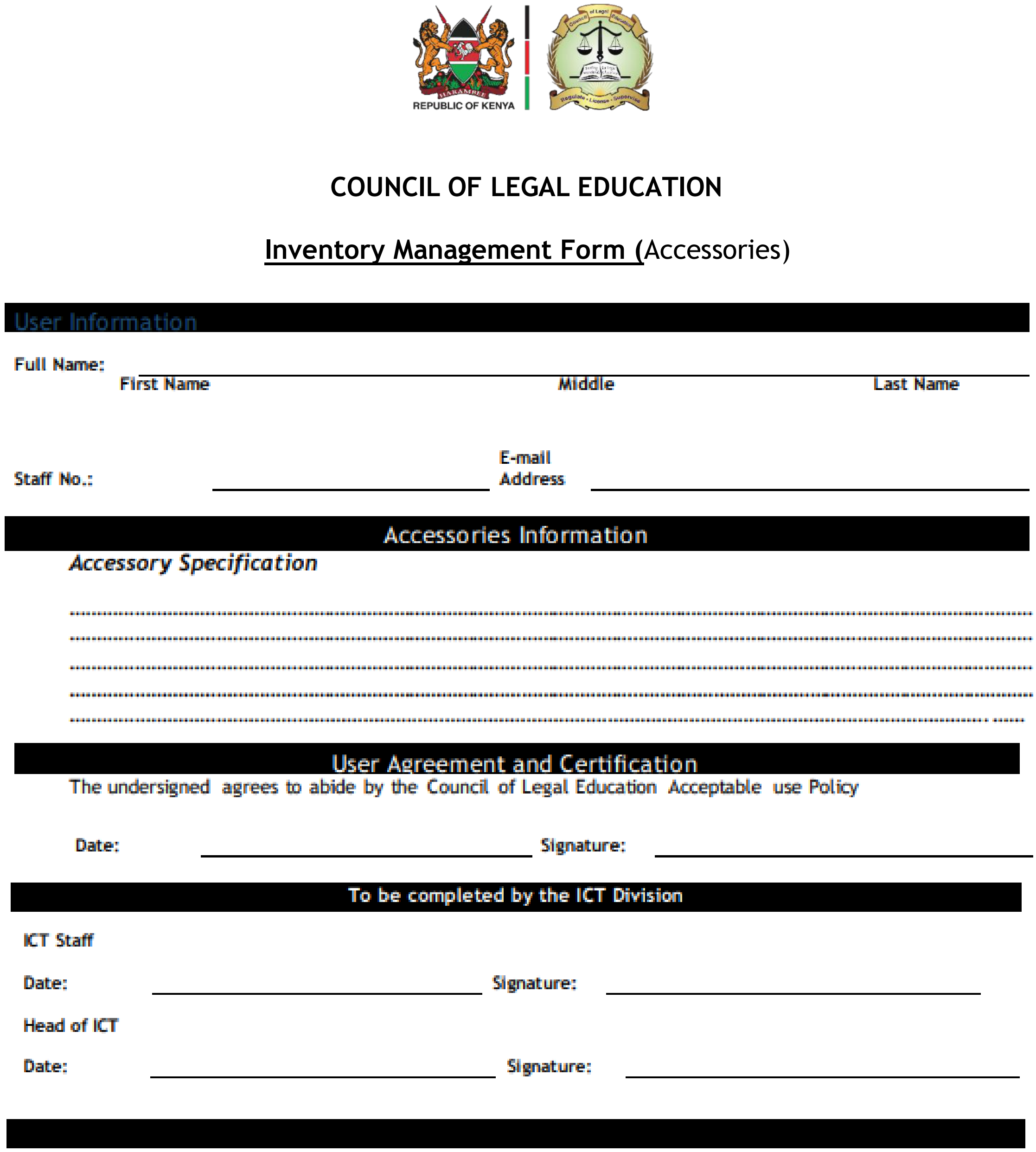
……

………

I hereby ***acknowledge*** that the computer & accessories are in good working condition

Name_______________ **Date**_______________ **Signature**_______________

6.2 APPENDIX II: Inventory Management Form (Accessories)



REPUBLIC OF KENYA

COUNCIL OF LEGAL EDUCATION

Inventory Management Form (Accessories)

User Information

Full Name: ____

First Name   Middle   Last Name

Staff No.: ____________________ E-mail Address ____________________

Accessories Information

Accessory Specification

....

....

....

....

....

User Agreement and Certification

The undersigned agrees to abide by the Council of Legal Education Acceptable use Policy

Date: ____________________ Signature: ____________________

To be completed by the ICT Division

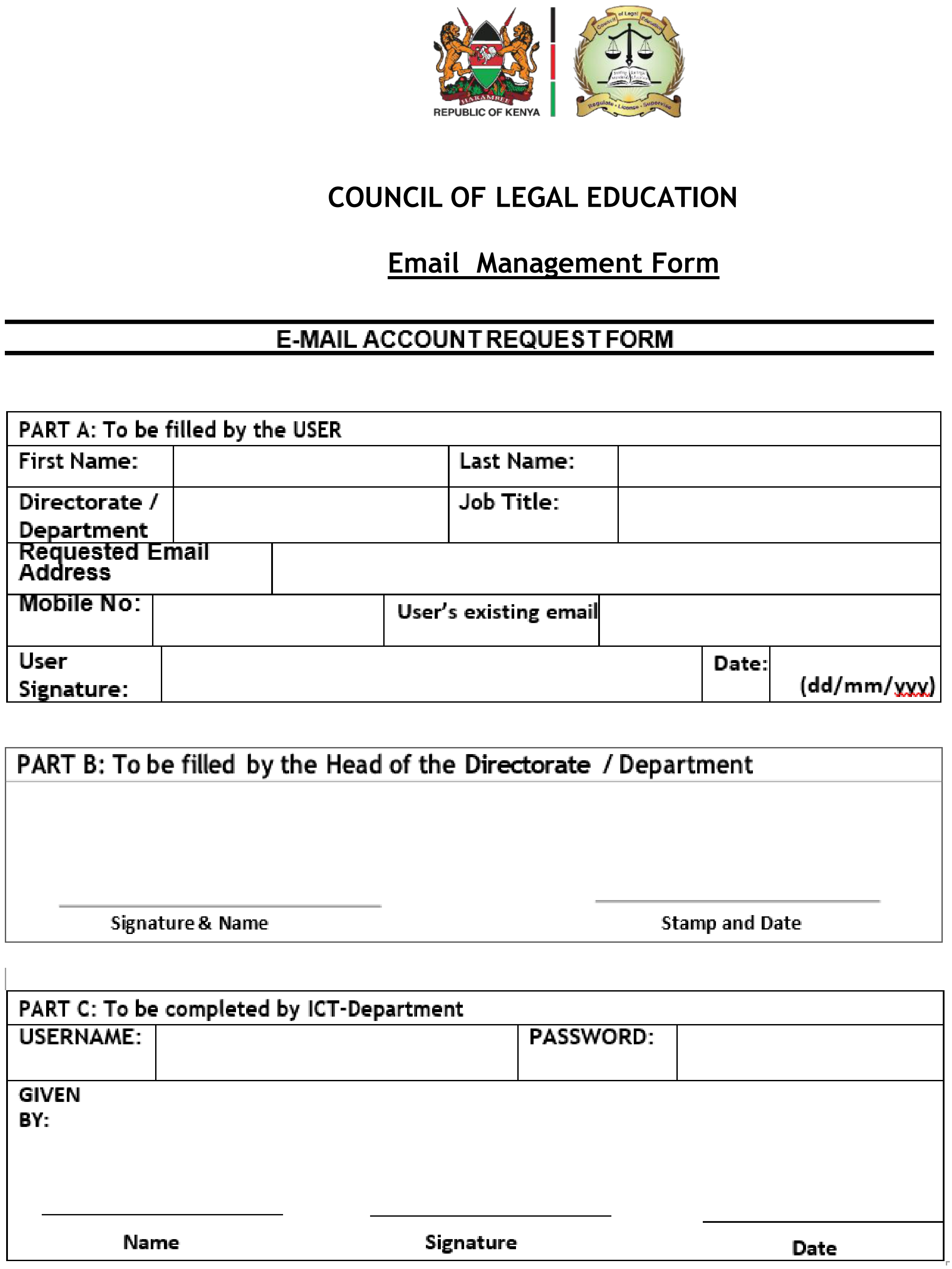
ICT Staff

Date: ____________________ Signature: ____________________

Head of ICT

Date: ____________________ Signature: ____________________

6.3 APPENDIX III: Email Management Form



REPUBLIC OF KENYA

COUNCIL OF LEGAL EDUCATION

Email Management Form

E-MAIL ACCOUNT REQUEST FORM

PART A: To be filled by the USER			
First Name:		Last Name:	
Directorate / Department		Job Title:	
Requested Email Address			
Mobile No:		User's existing email	
User Signature:		Date:	(dd/mm/yyy)

PART B: To be filled by the Head of the Directorate / Department

Signature & Name

Stamp and Date

PART C: To be completed by ICT-Department			
USERNAME:		PASSWORD:	

GIVEN BY:

Name

Signature

Date

6.4 APPENDIX IV: Change Request Form (CRF)

COUNCIL OF LEGAL EDUCATION

CHANGE REQUEST FORM (CRF)

CHANGE TITLE:

Provide a descriptive title for the change (indicate if the proposed change is related to an on -going project).

Change Category:

☐ Administration	☐ Operational	☐ Technical	☐ Auxiliary

Supporting Evidence Attached:

Please list be
low and attach to form.

Change Trigger(s):

☐ Stakeholder demand/observation
☐ Vendor recommended
☐ Accident/incident response
☐ Emergency/crisis situation
☐ Other (*State*):

Change Classification:

☐ Normal/Routine
☐ Emergency
☐ Other (*State*):

Request Submitted by:

____

____

On *(dd - mm - yyyy)*

____

Change Description:

Provide a detailed description of the proposed change.

Change Justification:

Explain why this change is needed.

Affected Stakeholders:

List stakeholders and describe how each will be impacted by the proposed change.

Expected Disruptions:

Detail any disruptions that will be expected from implementing the proposed change.

Desired Outcome:

Outline the specific outcome to be achieved by this change.

*** OFFICIAL USE ONLY ***

Receiving Dept.: ________________

Receiving Officer: ________________

Date Received: ________________

Reviewed By: ________________

Approval Status:

☐ Approved
☐ Conditionally Approved
☐ Hold for Future Action

Notes:

REPUBLIC OF KENYA

COUNCIL OF LEGAL EDUCATION

The Council of Legal Education,
P.O Box 829 - 00502,
Karen Office Park Karen,
Nairobi, Kenya.

020-6980100

info@cle.or.ke

0719150000

www.cle.or.ke