TEACHERS SERVICE COMMISSION

INFORMATION COMMUNICATION TECHNOLOGY (ICT) POLICY

(2020)

© **TEACHERS SERVICE COMMISSION**
P.O. BOX PRIVATE BAG-00100 NAIROBI
Email: info@tsc.go.ke
Website: www.tsc.go.ke

VISION

A Transformative teaching service for quality education.

MISSION

To professionalize the teaching service for quality education and development.

CORE VALUES

- **Professionalism**
- **Customer Focus**
- **Integrity**
- **Team Spirit**
- **Innovativeness**

ICT Vision

An effective Information Systems to support a transformative teaching service.

ICT Mission

To provide a secure, efficient and effective information systems while ensuring business continuity in professionalizing the teaching service.

First Published 2020

TABLE OF CONTENTS

FOREWORD

In undertaking its mandate, the Commission must embrace ICT in its processes and operations. This requires a well-developed technological investment, intelligent deployment and maintenance management plans to realise the value of the investment. In order to realise efficiency and effectiveness in the delivery of service, the Commission has deployed and continues to use ICT in its operations for strategic reasons. This calls for establishment of a comprehensive policy framework to provide direction on harnessing ICT in the Commission to realize its mandate.

The review of the ICT policy is, therefore, a milestone towards realisation of the TSC constitutional mandate by ensuring that ICT infrastructure and capacity are utilised optimally and are in line with its strategic objectives and relevant National Laws and Legislations on ICT. The Policy sets out the aims, principles and strategies for efficient service delivery which forms the basis for the development and integration of ICT in the Commission's operations and processes. Further, the Policy will enable the Commission to define the purpose of ICT while providing the opportunity to inform employees about the risks and rewards associated with its use.

The implementation of the Policy will enable the Commission to provide necessary and critical governance tool on ICT in a bid to ensure effective execution of its mandate through adoption of the latest technology. It will also help the employees to effectively participate in a rapidly changing world where work and other activities are increasingly transformed. It is my hope that the Policy will be instrumental to the realisation of the Commission's vision and mission by assigning responsibility for implementation and oversight.

Dr. Lydia Nzomo, OGW, CBS

COMMISSION CHAIRPERSON

PREFACE

Teachers Service Commission (TSC) has embraced Information Communication Technology in its operations to meet service delivery objectives of improving services and increasing productivity through ICT investment. Over the years, the Commission's operations have increasingly depended on ICT whose capacity has tremendously grown following successful automation of key services in the Commission. Systems have also been developed and deployed to offer online services to the teachers and third parties. The adoption and use of ICT has since created a considerable amount of investment in Information Systems to enhance processing, transmission and storage of information in the Commission.

All these developments require a comprehensive Policy to direct ICT adoption, acquisition, use and governance in the Commission. The purpose of this Policy is to ensure that the Commission's ICT related investment, operations, maintenance processes and usage are well directed to ensure that ICT services are in line with its business requirements based on existing Laws, Government Standards, Policies and best Practices. The Policy will guide the Commission in ensuring that all information resources and services are secured with appropriate controls and that all employees and other stakeholders use ICT facilities and services in a responsible manner.

The Commission takes cognizance of emerging risks and threats such as cyber-crime and misuse of computer technology. Therefore, there is need to ensure Business Continuity through ICT Disaster Recovery Plans, Computer security, cyber security and information security in the protection of computer systems and networks from theft or damage to the hardware, software, electronic data and from the disruption or misdirection of the services provided by the Commission. This Policy provides important control and governance tool necessary at this time of information-age where an organisation's data is such a critical Asset. It will also help the employees improve their capacity to perform duties.

The implementation of this Policy will enable the Commission to carry out its mandate in a more effective manner. All employees are, therefore, expected to embrace the use of ICT in their day to day operations. It is my hope that the Policy will guide the employees in providing quality services to the Customers and Stakeholders.

Dr. Nancy Njeri Macharia, CBS

COMMISSION SECRETARY/CHIEF EXECUTIVE

ABBREVIATIONS AND ACRONYMS

BCP	Business Continuity Plan
BYOD	Bring Your Own Device
CCTV	Closed Circuit Television
CIRT	Computer Incident Response Team
CIT	Contract Implementation Team
CRM	Customer Management System
DR	Disaster Recovery
DRP	Disaster Recovery Plan
EDMS	Electronic Document Management System
G2B	Government to Business
G2G	Government to Government
HRM&D	Human Resource Management and Development
HRMIS	Human Resource Management Information System
ICT	Information Communication Technology
IDEA	Interactive Data Extraction and Analysis
IP	Internet Protocol
IS	Information Systems
ISMS	Information Security Management System
LAN	Local Area Network
NDA	Non-Disclosure Agreement
NEMA	National Environment Management Authority
OLA	Operational Level Agreement

OSHA	Occupational Safety and Health Act
PLWDs	Persons Living with Disabilities
PPRA	Public Procurement Regulatory Authority
SCMS	Supply Chain Management Services
SLA	Service Level Agreement
SOP	Standard Operation Procedures
UPS	Uninterrupted Power Supply
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WAP	Wireless Access Point
WLAN	Wireless Local Area Network
VESDA	Very Early Smoke Detection Apparatus

DEFINITION OF TERMS

Term	**Operational definition**
Broadband	High speed Internet access with a wide bandwidth data transmission which transports multiple signals and traffic types.
Business Continuity Plan	A proactive plan to ensure that business processes continue during a time of emergency or disaster.
Computer Incident Response Team	A team that is assigned the responsibility for deterring, coordinating and supporting the response to a computer security event or incident.
Clean Power	Electrical power that is free from voltage spikes and drops.
Cloud Computing	On-demand availability of computer system resources especially data storage and computing power without direct active management by the user.
Compliance	Conformity with established ICT guidelines, specifications, relevant laws and regulations.
Data Centres	Physical or virtual infrastructure used by the Commission to house computer server and networking systems and components for Information Technology.
Disaster	An incident that causes damage, loss of life or property.
E-Government	The use of Information and Communication Technologies to offer services by the government.
Enterprise Architecture	A conceptual blueprint that defines the structure and operations of an organisation.

E-Waste Electronic and electrical devices discarded on or before the end of their useful life.

Government-to-Business An online non-commercial interaction between local and central government and the commercial business sector offering and exchange of services between government and businesses.

Government-to-Government Sharing of data and systems between government Ministries, Departments and Agencies.

Hardware Physical, tangible parts or components of a computer or computing systems.

ICT Facilities The Server rooms, Data centres, ICT operation rooms and any other room dedicated to ICT infrastructure and equipment.

ICT Governance Processes that ensure that an organisation's IT sustains and extends the organisation's strategies and objectives.

ICT Infrastructure Composite hardware, network, firmware, resources and services required for existence, operation and management of enterprise environment.

ICT Policy A top management document which guides ICT intentions and directions of the Commission.

ICT Project Management The process of planning, organising and delineating responsibilities for the completion of ICT goals in the Commission.

ICT Risk Assessment Overall process of risk identification, risk analysis and risk evaluation.

Information Systems Decommissioning The practice of discontinuing the usage and shutting down redundant or obsolete information systems while retaining access to the historical data.

Information Security Management System Documented management system that consists of a set of policies, processes and systems to manage risks to organisational data with the objective of ensuring acceptable levels of information security risk.

Management of Applications The Process of managing applications throughout their lifecycle.

Non-Disclosure Agreement A legal contract that prohibit a party from disclosing, sharing or using other than the intended purpose an entity's data or information that it may be given, discussed or come across during the period of its engagement.

Online Service A service provided over the internet.

Operational Level Agreement Internal Commission's agreements defined for internal users to meet Service Level Agreements.

Service Level Agreement A contract between a service provider and a client that documents the services provided while defining what the client will receive and clarifies what is expected of the service provider.

Service Provider An organisation or institution that offers ICT services to the Commission.

Software A set of coded instructions in the form of programmes that perform certain tasks using a computer's hardware.

Tier II Standard Data centre with VESDA, fire-suppression, raised-floor, false ceiling, environmental monitoring, CCTV monitoring, dedicated space for IT systems with a different room for power, dual UPS, dual cooling equipment, generator, dual-internet source, Uptime of 99.75%.

User A person who uses ICT application, equipment, facilities, processes or systems in their day to day operations.

1.0 INTRODUCTION

ICT advancements over the last few decades have led to its increased usage by organisations. It has impacted the way business is conducted, facilitated learning and knowledge sharing and general global information flows, empowered citizens and communities, resulting in a global information Society.

Internationally, United Nations Conference on Trade and Development (UNCTAD) has been helping countries in development and reviewing ICT Policies (UNCTAD, 2014). United Nations notes that ICTs are increasingly widespread in the world and are fast becoming the basis for economic development. UNCTAD in its paper Helping Countries Leverage ICT for Development pointed out that; the international community earlier on recognised their potential benefits and encouraged Governments "to elaborate, as appropriate, comprehensive, forward-looking and sustainable national e-strategies, including ICT strategies and sectoral e-strategies as appropriate, as an integral part of national development plans and poverty reduction strategies, as soon as possible and before 2010". A large number of developing countries have put in place one or several national ICT plans or are in the process of incorporating relevant policies and strategies into their national development plans (UNCTAD, 2014).

The high adoption of technology by organisations has brought the need to have a policy to guide ICT adoption, usage and acquisition by organisations. The public sector has not been left behind in adoption of technology and thereof the development of ICT policy. Vision 2030 Medium Term Frameworks had three pillars; Economic, Social and Political. ICT was identified as one of the key infrastructures to enable economic growth.

Kenya on August 7th, 2020 in The Kenya Gazette Vol. CXXII No. 150, gazetted the Nation ICT Policy guidelines, 2020. The Policy Guidelines has four objectives which cover: ICT Infrastructure development; Facilitation of Infrastructure and frameworks development; Contribution of ICT on GDP growth; Position the Country to take advantage of emerging trends by enhancing the education Institutions and the skills of the people; and Gain global recognition for innovation, efficiency and quality in public service delivery.

The Policy focuses on four areas with the fourth focus being Public Service Delivery. It is now a Government policy that all government services must be available online and that every Kenyan has online access and that government services are delivered quickly and fully at the time and place that they are needed. The ICT policy requires all arms of government to build, deploy, operate and manage locally built back-end and front-end systems to deliver services. This Policy also requires that Kenyan data remains in Kenya and that it is stored safely and in a manner that protects the privacy of citizens to the utmost. Government services are to be delivered in a manner that ensures the Country has a prosperous, free, open and stable society.

Teachers Service Commission developed ICT Policy 2010. It is this Policy that is being reviewed to address the changes in technology, its adoption and other emerging technological issues. This Policy will be used to provide a comprehensive framework to support and ensure that logical access controls are implemented appropriately to protect information technology resources in accordance with the Commission's information security requirements. It is also to provide guidelines on usage and utilization of the Commission's ICT resources.

1.1 RATIONALE

The dynamic nature of technology and the significant continued absorption of ICT use in the Commission to improve service delivery calls for the review of its ICT Policy 2010 to resonate with these requirements. Rapid technological changes, changing public needs, legal framework and evolving ICT global trends require a policy to provide a suitable anchor. In order to provide a clear guidance on the acquisition, development and use of the ICT resources in the Commission while offering the required protection to the Commission Information Assets, it was necessary to develop this policy.

2.0 POLICY STATEMENT

The Commission is committed to creating an enabling environment for promotion and use of ICT in the provision of services in a manner that is ethical, efficient, effective and lawful. The Commission will continuously enhance its organisational capacity by adopting modern technology and skills development.

3.0 AUTHORITY

The policy derives its authority from:

(i) The Constitution of Kenya.

(ii) TSC Act (2012).

(iii) Kenya Information and Communication Act (2012).

(iv) Access to Information Act (2016).

(v) National ICT Policy (2016).

(vi) The National ICT Guidelines (2020).

(vii) National E-waste Policy (2018).

(viii) Public Procurement and Asset Disposal Act (2015).

(ix) Public Procurement and Disposal Regulations (2020).

(x) Computer Misuse and Cybercrimes Act (2018).

(xi) Data Protection Act (2019).

(xii) OSHA Act (2007).

(xiii) Government ICT Standards ICTA-2019.

4.0 POLICY OBJECTIVES

4.1 General Objective

To provide principle direction in the use of ICT in the Commission's operations, investments, maintenance and processes for effective service delivery.

4.2 Specific Objectives

The specific objectives of this policy are to:

(i) Regulate acquisition, implementation, maintenance and use of ICT resources in the Commission.

(ii) Improve security of Data, Information and ICT Assets in the Commission.

(iii) Promote innovation and use of technology to improve service delivery.

5.0 SCOPE

This Policy applies to all TSC employees, users, ICT suppliers, contractors and service providers.

6.0 POLICY PRINCIPLES

The Policy shall be guided by the following key principles:

(i) Seamless integration of ICT systems.

(ii) Adherence to international ICT standards and best practices.

(iii) Security, integrity and reliability of data and information systems.

(iv) Transparency and accountability in service delivery.

(v) Innovation and ease of doing business.

7.0 POLICY GUIDELINES

This Policy will be implemented through the guidelines as outlined in the **ANNEXES**.

7.1 ICT Governance

The Commission shall be responsible for ICT strategic decisions to ensure that all ICT projects and initiatives deliver value to the Commission. The Commission shall use E-governance guidelines.

A three-year permanent Strategic IT Committee (SITC) with the responsibility for the overall strategic management and monitoring of ICT resources utilisation and key ICT projects progress in the Commission shall be established. The Committee shall comprise six members appointed and chaired by the Commission Secretary with the Director ICT as the Secretary. The responsibilities of this governance Committee are as indicated in **Annex I.**

7.2 ICT Operation Structure

The ICT function shall operate as a Directorate as per the Commission Management Structure. End user Directorates and Sections shall be responsible for day-to-day data input and operations of the specific information systems in the directorate. The Commission shall:

(i) Set up an ICT governance model with appropriate structures to manage ICT Operations.

(ii) Establish clear roles and responsibilities for the ICT governance structure.

(iii) Identify and appoint qualified Staff.

7.3 ICT Infrastructure

The Commission shall establish and continuously improve standards on installation, security, management, use and implementation of ICT infrastructure in all service delivery points/locations. The guidelines shall address four (4) key areas namely; ICT Networks, ICT Facilities, Power provisions and equipment as provided in **Annex II.**

7.4 ICT Information Systems

The Commission shall provide guidelines on the acquisition of appropriate software in terms of use, value for money, scalability, integration with existing and future systems in the Commission. The systems will be used, operated and managed efficiently to ensure effective service delivery. The detailed guidelines are as indicated in **Annex III.**

7.5 ICT Service Management

The Commission shall ensure availability of ICT services as provided for in the Operation Level Agreements (OLAs) and Service Charter through a centralised management unit responsible for support of all ICT services.

The ICT Directorate shall develop an Operational Level Agreement (OLA) stipulating its commitment specific to each process owner. This will help to monitor and manage the quality of ICT services in the Commission. The detailed guidelines are as indicated in **Annex IV.**

7.6 Data and Information Security

The Commission shall secure its data and information against breaches and threats by preserving its Confidentiality, Integrity and Availability. A vulnerability assessment and penetration testing of all systems and infrastructures shall be undertaken on a bi-annually basis and reports presented to the Strategic IT Committee (SITC). The detailed guidelines are indicated in **Annex V.**

7.7 Business Continuity Plan

The Commission shall develop and maintain a Business Continuity Plan with DRP specific to ICT which will include critical information systems, ICT Infrastructure and Information Assets as indicated in **Annex VI.**

7.8 Cloud Computing Services

Cloud Computing is a concept that refers to services, applications, and data storage delivered online through powerful file servers interconnected through the internet infrastructure. It allows consumers and businesses to use applications without installation and access their data and information at any computer with internet access. The Commission's take-up on the use of Cloud Services shall be approved on a case by case in-line with existing government standards, policies and guidelines. The guidelines to be applied shall be as indicated in **Annex VIII.**

7.9 Electronic Waste (E-WASTE)

All obsolete and unserviceable ICT equipment shall be disposed of in accordance with relevant NEMA E-Waste Regulations and the relevant Public Procurement and Asset Disposal Act.

7.10 Data Management

Retention and disposal of data no longer with special reference to regulatory requirements and business need shall be disposed of as per the Commission Records Management Policy.

8.0 POLICY IMPLEMENTATION

The Commission shall use the existing administrative structures to implement this Policy.

0.9 MONITORING AND EVALUATION

This Policy shall continuously be monitored and evaluated in line with the existing Monitoring and Evaluation Guidelines of the Commission.

10.0 POLICY REVIEW

The Policy shall be reviewed after every three years or as the need arises to align it to government policies, legal requirements and any emerging issues as the Commission may deem appropriate.

11.0 RISKS

The risks associated with the implementation of this Policy are as indicated in **Annex IX.**

12.0 ICT EQUIPMENT ALLOCATION MATRIX

Distribution of end-user computing equipment shall be as per **Annex X.**

13.0 POLICY ENFORCEMENT

Failure to comply with this Policy, standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment as per the HR Manual for employees or termination of contracts for contractors, partners, consultants and other entities. Legal action also may be taken for violations of applicable regulations and laws.

ANNEXURES

ANNEX I: STRATEGIC IT COMMITTEE (SITC)

1. ESTABLISHMENT

A six-member Strategic IT Committee (SITC) which shall serve for three (3) years shall be established and headed by the Commission Secretary or a representative.

2. RESPONSIBILITIES

The SITC will be responsible for overseeing the development, implementation and monitoring of the ICT policy, strategy, projects prioritisation and execution, and governance matters.

2.1 In undertaking these responsibilities, the SITC will:

(i) Recommend and/or approve medium and large projects of strategic importance to the Commission's Strategic Plan and ensure a strategic balance.

(ii) Review major project risks including; Disaster Recovery, Audits and advisory on IT related Projects.

(iii) Co-ordinate IT project prioritisation based on programme priorities to inform the Commission's planning and budget cycle, provide regular reports and present business case budgets and priorities for strategic IT projects to Commission Board Committees.

(iv) Determine major action including the suspension of Projects.

(v) Develop annual Cycle of IT Governance business which includes: discussion on emerging strategic IT issues; regular review and approval of the Commission's IT Risk Register; review of reports from the ICT Director on Commission's ICT Business Continuity and Disaster Recovery plans and procedures and review reports on ICT security.

(vi) Review of reports on IT related items identified by internal or external audit reports to ensure timely resolution.

(vii) Review and lead continuous improvement on IT Governance matters across the Commission.

2.2 MEMBERSHIP

The membership of the Strategic IT Committee will consist of:

(i) Commission Secretary (Chair).

(ii) Director ICT (Secretary).

(iii) Four other members as shall be appointed by the Commission Secretary.

2.3 INVITEES

The SITC may invite any person or persons, whether from within or external to the Commission, to its meetings as it may determine to assist in its deliberations either on a particular item or for the whole meeting.

2.4 REPORTING

The SITC reports to the Commission Management.

2.5 REVIEW OF THE COMMITTEE

The SITC will review its functions and performance at a minimum every year.

2.6 FREQUENCY OF MEETINGS

(i) The Strategic IT Committee will meet at a minimum four times a year with at least one meeting in each quarter.

(ii) Meetings will generally be scheduled at least one quarter in advance to align with the Commission's planning cycle.

2.7 QUORUM

The quorum for meetings of the Strategic IT Committee is a half of the membership with prior-approval from the Chair of the agenda.

2.8 DECISIONS

Decisions shall be through consensus.

ANNEX II: GUIDELINES FOR ICT INFRASTRUCTURE

Network Management

The network shall be set up in all TSC Offices and managed in adherence to the standards outlined in the following guidelines:

(i) The network shall consist of the Local Area Network (LAN),Wide Area Network (WAN) and Wireless Local Area Network (WLAN).

(ii) Emphasis shall be on the adoption of secure networks in deployment of the network infrastructure.

(iii) The devices in the network ecosystem shall include but not limited to; computers, devices that support the flow and processing of information, ICT datacentre, telephone systems and related software.

(iv) The ICT Directorate shall: -

(a) Maintain a clear network layout diagram of all TSC premises for purposes of reference, maintenance, support, expansion and business continuity.

(b) Monitor the utilisation of the network infrastructure and advise on future expansion and security in line with international standards and best practice.

(c) Periodically review technical specifications, configuration and installation guidelines to ensure conformity and compatibility with existing infrastructure.

(v) Only approved network connectivity devices by ICT Directorate shall be allowed to transmit signals to connect the Commission's equipment within TSC premises.

(vi) Access to TSC Server rooms and network cabinet installations shall be restricted to authorised personnel.

(vii) The Commission reserves the right to monitor internet usage and block sites or users to ensure security and integrity of its data assets and any other resources.

ICT Facilities

ICT facilities include; the server rooms, datacentres, operation rooms and any other room dedicated to ICT infrastructure and equipment in the Commission. The following guidelines shall apply:

(i) All Infrastructure projects including new construction and refurbishment shall include approved designs for ICT installation as part of the scope of works for the projects.

(ii) Data centres shall house all servers core network equipment and shall be provided with; uninterrupted power supply (UPS), air conditioning, Very Early Smoke Detection Apparatus (VESDA), Fire Suppression, CCTV Monitoring, Humidity and Water Monitoring Instrument and Access Control and Notification Systems.

(iii) Equipment rooms and locations shall have Network cabinets and associated equipment necessary for distribution of TSC network.

(iv) There shall be facilities to house Major Uninterrupted Power Supply (UPS) equipment.

(v) ICT facilities shall be optimally located within the TSC premises. Such a location shall consider factors including but not limited to security, fire resistance, noise, heat and electricity supply.

Power Provision

ICT facilities and equipment require a stable power provision to prevent failures or inaccessibility of online services. The following guidelines shall apply:

(i) The Head of ICT Directorate, in consultation with the responsible implementing Unit (s), shall ensure that TSC Offices are installed with adequate backup power supply.

(ii) All active critical ICT infrastructure shall be connected to clean power.

(iii) All users/process owners shall seek authorisation from designated ICT Officers to alter, repair or replace such power installations.

(iv) The UPS shall be used to power ICT equipment only.

(v) Other electrical appliances such as, water heaters, electric kettles, water dispensers, microwave ovens and electric fans shall only be connected to regular power.

Management of ICT Equipment

These guidelines apply to specifications, requisition, procurement, allocation, distribution, asset register, maintenance, use and disposal of ICT equipment in the Commission. All equipment remain the property of the Commission and users must take care of the equipment under their custody and use.

(a) Requisition

(i) The requisition for all ICT equipment and accessories shall be made by the respective Heads of Directorate, Division and Section and County Directors through ICT Director.

(ii) The ICT Director shall from time to time review and consolidate such requisitions, confirm they are required and prepare technical specifications and requirements for each item.

(b) Acquisition

The ICT equipment may be acquired through purchase or donations.

(i) The procurement and delivery of ICT Equipment shall be guided by existing laws and government procurement regulations.

(ii) Donated ICT equipment shall be accepted upon meeting minimum specifications or on advice by the ICT Director.

(c) ICT Equipment Asset Register

The ICT Directorate shall maintain an ICT asset register for monitoring the issuance, usage, surrender, movement, maintenance and loss of ICT equipment acquired by the Commission.

(i) The register shall contain details of all ICT equipment.

(ii) The ICT Officers shall conduct quarterly inventory audit of the equipment and submit a report to the ICT Director.

(iii) The equipment that is no longer in use shall be surrendered to the ICT Director for redistribution or recommendation for disposal.

(d) Allocation and Responsibility

(i) The ICT equipment shall be allocated to an individual employee in accordance with the ICT Equipment Allocation Matrix **Annex X.**

(ii) The ICT Director shall ensure that ICT equipment issued to staff match the nature of their work.

(iii) The user issued with an ICT equipment shall fill ICT Equipment Acknowledgement Form **Annex XI.**

(iv) The ICT Directorate shall ensure that all ICT equipment are standardised for ease of maintenance

(v) Users who require specialized equipment shall submit a written request to the ICT Director for advice and consideration.

(vi) Any officer issued with a new or replacement equipment shall surrender the old one immediately after inspection by the ICT Director for update of the inventory.

(vii) ICT Officers and users shall ensure that data from the surrendered machine is backed up or transferred to new equipment where necessary.

(viii) ICT Director shall distribute ICT equipment in consultation with the Commission Secretary.

(e) Issuance of ICT Equipment

(i) Officers to be issued with ICT equipment shall be required to sign the ICT Equipment Issuance Form from ICT Directorate.

(ii) All Users and Employees shall be responsible for equipment issued to them.

(iii) Non-employees of TSC shall only be issued with ICT equipment upon approval by the Commission Secretary.

(f) Custody of ICT Equipment

(i) The custody of all ICT equipment shall be done in collaboration with the SCMS Division under the guidance of the Commission Secretary.

(ii) The ICT Equipment shall only be moved from the current station with the authority of the ICT Director after filling the ICT Asset Movement Form.

(iii) An Employee on secondment to other Institutions shall surrender all equipment in their possession as prescribed in the clearance procedure.

(g) Security and Loss of ICT Equipment

(i) Necessary precaution shall be taken while using ICT equipment out of TSC premises. Failure to demonstrate due diligence in protecting equipment shall constitute negligence and the user shall be held liable for the loss.

(ii) Loss of ICT equipment must be reported immediately to the nearest police station and an abstract obtained. Thereafter, the loss must be reported to the Commission Secretary using ICT Lost-Damaged Equipment Reporting Form in **Annex XI.**

(iii) ICT Director shall regularly carry out awareness on Information Security.

(iv) All employees must be aware that any loss of data held in ICT equipment exposes the Commission to serious security lapses. All necessary measures must therefore, be taken to protect the data in the devices.

(h) Maintenance of ICT Core Infrastructure

(i) Manufacturers' warranties shall be diligently managed for core ICT infrastructure. Maintenance contracts and Service Level Agreements shall be in place for core equipment at all times.

(ii) The Directorate of ICT shall perform scheduled maintenance of core ICT infrastructure.

(iii) The Head of ICT Directorate shall prepare a technical report with recommendation for decommissioning non-performing core ICT infrastructure in readiness for disposal.

(i) Acceptable use of ICT Infrastructure

Acceptable use of ICT infrastructure entails appropriate and responsible use of such facilities in the dispensation of TSC Services. The following guidelines shall apply:

(i) ICT infrastructure shall not be used for personal activities.

(ii) Unauthorised connection of monitoring devices/equipment to the TSC ICT infrastructure is prohibited.

(j) Data Center Security

The ICT Director shall ensure that Data Center /Server Room facilities are:

(i) Located in secure locations.

(ii) Meet Data Centre Tier II Standard requirements or above.

(iii) Ensure anyone wishing to access the Data Center fills a Data Center Access Form **Annex XI** after reading and signing the Teachers Service Commission Data Center Rules and Regulations **Annex XI**.

(k) Provision of Internet Services

The following guidelines shall apply in the provision of Internet Services:

(i) The Commission shall provide Internet Services and resources to facilitate service delivery.

(ii) The Internet Services and Resources shall be exclusively used for Commission's service delivery.

(iii) The Commission reserves the right to monitor internet usage.

(iv) The User shall not use the Internet for;

(a) Personal use or gain.

(b) Disseminating or printing copyrighted material in violation of copyright laws.

(c) Carrying out activities that could cause congestion and disruption of TSC network and systems.

(d) Inappropriate and unlawful content.

(v) The use of the internet shall conform to the TSC Code of Conduct and Ethics.

(vi) The Commission reserves the right to provision of internet utility which is also subject to budgetary allocation.

(vii) The Commission reserves the right to block sites and users from internet access as it may deem appropriate.

ANNEX III: INFORMATION SYSTEMS

The Commission's Information Systems are implemented for the sole purpose of improving the effectiveness and efficiency of service delivery. These Information Systems may have major impact on corporate strategy and organisational success. Thus, require involvement of management in all aspects.

Information Systems Development

The development of Information Systems for the Commission will follow the approved open standards and methodology.

Information System Database and Backups

The Commission's data is very critical for decision making hence, the need to ensure the data repositories are secured and backed up for restoration in case of disaster or logical errors. The Commission shall backup its information systems and databases.

General Requirements

The Commission shall:

(i) Determine whether to develop or acquire a required Information System(s).

(ii) Ensure that the Information System is operational, well maintained and sustainable.

(iii) Ensure all software is strictly used for Commission's purposes only.

(iv) Ensure the Information Systems meet approved quality standards.

(v) Ensure process owners consult with ICT Director on matters of;

  (a) Integration of ICTs into their processes.

  (b) Implementation of specific components of the ICT Policy and Strategy that support their processes.

  (c) Ensure compliance with the ICT Policy.

(vi) Establish a strategy for managing changes in the Information System for new deployment.

Information Systems Acquisition

The following procedure shall apply in the acquisition of ICT Information Systems:

(i) Acquisition and or applications shall be done in accordance with the provisions of the relevant procurement law.

(ii) A detailed business and system requirement shall be established before any application or acquisition.

(iii) Specifications shall be developed to guide in the selection of competent suppliers.

(iv) The operating environmental conditions must conform to the minimum manufacturers' specifications and best practices.

(v) Capacity building and transfer of knowledge of deployed Information System shall be conducted by the supplier before a completion certificate is issued.

(vi) Process owners shall be involved in the acquisition, implementation of new systems and training of staff upon installation. User acceptance shall be provided for all new Information Systems installed.

(vii) Ensure compliance with best practice for any system being acquired.

(viii) Upon successful installation of any Information System, a Completion Certificate duly signed by the Commission Secretary shall be issued.

(ix) User and Technical Manuals shall be part of the minimum requirements for all systems acquired or developed by the Commission.

Information Systems Development

The following guidelines shall apply in the development of Information Systems in the Commission:

(i) Information Systems developed in-house shall be a property of the Commission.

(ii) The platform and database to be used shall be approved by the ICT Director.

(iii) The ICT Director shall ensure that backup and recovery procedures for each system are documented and periodically reviewed.

(iv) System design must be approved by the ICT Director and the process owner before a system development.

(v) Final system source codes shall be surrendered to the Commission through the ICT Director.

(vi) System codes, configurations data and installation kits shall be backed up.

Information Systems and Software Maintenance

Information System and Software Maintenance include any activity which requires use of an information system for the purpose of upgrading, reconfiguring, modifying, replacing, changing or servicing within a given period of time. Maintenance includes, but are not limited to, software changes, hardware changes, patches, fixes and updates. The following guidelines shall apply:

(i) The ICT Director shall advise the Commission on Information Systems and Software Upgrades.

(ii) Information Systems and Software shall be maintained regularly to ensure compliance with the changing requirements of the Commission and technological changes.

(iii) New Information Systems and Software shall be installed and tested in the test environments based on the information systems testing procedure as indicated in *(Information Systems Testing)*.

(iv) A **System Change Request Form - Annex XI** shall be filled, duly signed and approved for any change to be elected.

(v) The System Administrator shall schedule systems maintenance at an appropriate time with a prior notice and approval from ICT Director accordingly.

(vi) Applicable system maintenance logs and documentation shall be updated and reviewed after maintenance.

Information Systems Testing

The following guidelines shall apply in the testing of an Information System:

(i) Different aspects of the System shall be tested such as, response to time, boundary data, no input and heavy volumes of input.

(ii) The Programmer who develops the system will not be the one to perform the testing.

(iii) Standard debugging tools shall be used.

(iv) A Test and Quality Checklist shall be maintained indicating the test results.

(v) The process owner shall be involved in the testing of the system.

Information Systems Documentation

The following guidelines shall apply in the documentation of Information Systems:

(i) Every Information System shall have the following documents;

(a) System Documentation.

(b) User Manual.

(c) Training Manual.

(ii) The standard for the documentation shall be comprehensive, informative and well structured.

Information Systems Monitoring and Evaluation

(i) ICT Director together with the process owners shall conduct monitoring and evaluation of systems after every 2 years to determine areas of improvement on all systems.

(ii) User satisfaction survey shall be conducted annually to establish success of the Information Systems.

Information Systems Decommissioning

The Commission shall ensure that all systems commissioned have a predetermined lifespan. A review shall be done in every two years to determine the system usage, continuity, discontinuity or decommissioning.

At the end of life, a changeover or replacement, the Information System shall be decommissioned. When decommissioning a System, the Commission shall ensure that existing data is protected and stored for future use and made available as required.

The following guidelines shall apply:

(i) A System shall be analysed for usefulness and its need.

(ii) Once an Information System, Application and/or Database reaches its end-of-life, a Service Area may seek to decommission the System, Application and/or Database by making a formal request to ICT Director.

(iii) When decommissioning an information System, Application and/or Database, records retention policies may require that the records contained within the information System, Application and/or Database be retained beyond the useful life of the Information System, Application and/or Database.

(iv) There shall be a last backup done as per the Systems Backup Guidelines.

Software

The following guidelines shall apply to all Software in the Commission:

(i) Establishment of appropriate Software Standards to facilitate acquisition and development.

(ii) Approval of the Software by the ICT Director prior to acquisition, download, installation and use is required. Any Software serving a specific Service Area, the process owner shall, together with the ICT Director issue the approval.

(iii) Proprietary Software must be licensed throughout their life and where necessary supported.

(iv) Open Source, Shareware or Freeware Software must be compatible with the Commission's Hardware and Software Systems.

(v) Commission users shall use Software in conformity to copyrights laws, terms of licensing and use.

(vi) The Commission shall endeavour to use Software that do not require licensing or use one-off licensing and use Open Standard Architecture.

User Accounts

The following guidelines shall apply for employees' User Accounts:

(i) Employees shall make formal requests for a User Account by filling the System

Access Request Form. The Form shall be recommended by their immediate Head of Service Area and approved by Head of ICT Directorate.

(ii) User Accounts shall be uniquely created.

(iii) User Accounts that are unused shall be disabled.

(iv) Users shall be granted privileges that are commensurate to their roles and responsibilities.

(v) All other Users but not limited to Contractors, Vendors, Attachees and Interns can be given access at the discretion of the Commission Secretary.

Email Services

The following guidelines shall apply for Email Services:

(i) Official Communication shall be done through the TSC e-mail System.

(ii) Personal Emails shall not be used to transmit Commission's Official Communication.

(iii) Email Accounts shall have storage quotas which are defined and managed centrally.

(iv) Email shall not be used to send chain e-mails that generate unnecessary high-volume traffic.

(v) Users shall not reply to unsolicited e-mails received.

(vi) Automatic forwarding of TSC Email to personal external Email Addresses is prohibited.

(vii) Information transmitted by Email shall not be defamatory, abusive, involve any form of racial or sexual abuse, contain any material that is detrimental to any party or is outside the specific business interests of the Commission.

TSC Website

The Commission acknowledges the importance of Website in Communication. The following guidelines shall apply:

(i) The TSC Website shall be hosted and managed by the Commission.

(ii) The day-to-day running of the website shall be done by the Corporate Affairs Division while ICT Directorate provides the Technical Support.

(iii) Website content shall be informative and updated.

(iv) Web Pages shall undergo professional scrutiny and careful preparation before publishing.

(v) The Heads of Service Areas shall be responsible for the content of published Pages and are expected to abide by the highest standards of quality and responsibility.

(vi) The Webmaster shall ensure that the Website and Pages comply with appropriate Policies, Branding and Standards as well as applicable Legal Requirements.

Social Media

The use of Social Media is covered by the TSC Communications Policy.The Commission's Social Media Activities shall be handled by the Corporate Affairs Division.

Issuing, Suspension and/or Termination of System Access Privileges

Process Owners shall issue rights to the Systems under their usage by approving the **Systems Access Request Form** for their requesters. ICT Directorate shall only be charged with the System Administration aspect of Information Systems.

User access to Information Systems shall be Terminated when:

(i) An Employee who is a System user exits employment.

(ii) An Employee is on suspension or temporary detachment from the Commission.

(iii) There is a breach of terms of use on any of the Systems.

(iv) The process Owner requests for such suspension and/or termination.

(v) Accounts not used for a 90-days period for active Systems shall be disabled and deactivated after six-months.

Systems Backup

Information Systems shall be backed up regularly to ensure Information Systems, Data and Software can be recovered in case of an incident. The following guidelines shall apply:

(i) System Administrators shall establish and formally document an appropriate Register and Schedule for full and incremental backups.

(ii) Backup Copies shall be retained on a Yearly, Monthly, Weekly and Daily basis.

(iii) Back-up Data must be given a level of physical and environmental protection, consistent with standards applied in the Disaster Recovery Plan.

(iv) If Data is lost due to logical errors, the Database must be recovered up to the nearest possible useful point before the error occurred.

(v) After the loss of Data, the recovery time will consist of time for: Analysing the error; Replacing the required hardware, setting up the operating system and required file systems; Restoring the Database from the data backups; and Performing an instant recovery automatically at system start-up.

(vi) Additional backups shall be taken immediately before and after structural change to the Database and/or Operating System's File so as to ensure successful restoration in the event that the Database or System crash (failure) occurs after the structural change and before scheduled backup.

(vii) All Systems will be backed up as per the backup Schedule maintained by the Deputy Director ICT (Systems and Innovations).

(viii) Periodic restores will be done regularly on the test environment to ensure correctness and integrity of the backup.

The following information shall be documented for all generated Data Backups: Date and time the data backup was carried out (dd/mm/yyyy: hh:mm); The name of the system or short description of the nature of the data; Extent and type of data backup (files/directories, incremental/full); Backup hardware and software used (computer name, operating system (OS), version number); Physical location of the server and the logical path on file-system to the back-up area when fixed media (hard-disks) are used; and Data backup and restoration procedures shall be guided by the Standard Operation Procedures (SOP).

ANNEX IV: ICT SERVICE MANAGEMENT

ICT Service Management is concerned with the management and delivery of ICT resources and core business practices to give end users support for the most desired results in carrying out their day to day activities. The following guidelines shall apply:

1. ICT Help Desk

In an endeavour to minimise disruptions in the provision of ICT Services, the ICT help desk shall ensure that;

(i) ICT incidents and service requests are reported through the System and/or email.

(ii) All incidences must be put into the Helpdesk System and a Ticket Number issued.

(iii) Response to queries is done within the stipulated timeframe outlined in the Service Charter and that ICT related issues are resolved promptly.

(iv) Service Requests are allocated resolution time and an ICT Officer to resolve.

(v) All the Tickets are resolved within stipulated timeframe or escalated to the next level and necessary feedback communicated to the user.

(vi) Regular Reports from the Helpdesk System shall be shared with the Commission Secretary on a Monthly basis.

2. Training

The ICT Director shall conduct ICT training and development for ICT users. The following guidelines shall apply:

(i) The ICT Director in conjunction with Director (Human Resource Management and Development – HRM&D), shall carry out needs analysis to identify ICT skill gaps.

(ii) The ICT Director in conjunction with D(HRM&D), shall identify and allocate necessary budgets and prepare the training venue(s) and materials for internal training.

(iii) All trainings conducted through ICT Directorate shall have a summative evaluation and a training Report which shall be sent to the D(HRM&D).

(iv) Systems Users shall receive training for new and existing Information System Software.

3. ICT Service Centre

The ICT Directorate shall establish an ICT Support Service Centre to be run and maintained under Service Management. The following guidelines shall apply:

(i) The Directorate shall Operate a maintenance workshop for ICT equipment.

(ii) Faulty or damaged equipment shall be reported or delivered to the Service Centre using the ICT Asset Movement Form.

(iii) A complete backup of Data shall be done on ICT equipment that requires major repairs.

(iv) Any faulty equipment shall be diagnosed for identification of fault(s). The identified faults shall be logged and rectified within the stipulated time in accordance with the ICT Service Charter.

(v) In a case where a Technical Officer is unable to repair the equipment, he/ she shall escalate the issue to the immediate supervisor or the contractor responsible for maintenance for a resolution within the stipulated timeframe.

(vi) Broken-down ICT equipment shall be declared as damaged if assessed and found to be no longer functional.

(vii) Service Management shall notify the User once the equipment has been repaired.

(viii) ICT equipment shall have a recommended usage lifespan of five (5) years to be replaced subject to availability of funds.

4. Operational Level Agreements (OLA)

The following guidelines shall apply for Operational Level Agreements:

(i) The ICT Director shall establish and maintain Operational Level Agreements (OLA) with Heads of Service Areas on ICT services offered.

(ii) Annual OLA Reports shall be prepared and submitted to management by SITC.

(iii) OLA monitoring and evaluation shall be carried out by SITC.

5. Service Level Agreement (SLA)

The Service Level Agreement shall be guided by the following:

(i) The Director ICT shall establish and maintain Service Level Agreements with third party providers offering ICT services.

(ii) The Service Level Agreement shall describe the responsibilities of both parties, penalties and specifications outlined in the scope before commencement of ICT project.

(iii) The monitoring process and reporting of Service Level Agreement shall be established.

(iv) All documentation of ICT projects undertaken shall be kept under a safe custody by Director ICT.

(v) Information regarding Service Level Agreement for all Systems and Software maintained by Contractors shall form part of the contract and a copy kept by Director ICT.

6. Management of ICT Service Providers

The Director ICT shall co-ordinate the activities carried out by all ICT Service Providers to ensure services offered meet the business needs of the Commission. The following guidelines shall apply:

(i) The Director ICT shall ensure cordial working relationships are established and sustained with the Service Providers.

(ii) A monitoring and reporting mechanism on performance of the Service Providers shall be established as per the Service Level Agreement.

(iii) Service Providers Personnel carrying out works in the Commission shall be provided with TSC Temporary Identification Cards that shall be put on at all times while at the Commission Premises.

(iv) The Temporary Cards shall be surrendered back to the Commission on completion of the task being undertaken.

(v) The Service Providers shall provide all the necessary clothing and tools for their staff in compliance with OSHA.

(vi) The Service Providers shall provide their staff with dust-coats with their company logo which shall be worn at all times when at the Commission Premises.

7. ICT Projects Management

In order to ensure only viable projects are implemented, ICT Projects shall be approved by the Commission Secretary on advice from the Strategic IT Committee (SITC). SITC shall monitor the implementation of all major ICT Projects and advise the Commission Secretary. For the day-to-day running of Complex ICT Projects, the Commission shall establish a Contract Implementation Team (CIT) as per the Procurement law with the responsibility to monitor and implement the ICT Projects. The ICT Directorate, together with the user Directorates, shall play a leading role in the management of these Projects with the Head of ICT responsible for:

(i) Ensuring that all projects undertaken conform to the Government's ICT Project Management Procedures.

(ii) Preparing and maintaining technical project documentation that include but not limited to project Plans, Schedules, Budget and the risk analysis in consultation with the contractor and CIT.

(iii) Ensuring compliance with all internal procedures for managing projects.

(iv) Establishing a reporting mechanism to ensure implementation of projects within the specified timelines and budget provisions.

(v) All other non-complex ICT Projects shall be carried out by the Director ICT.

8. Hardware Maintenance

In order to minimise downtime and ensure continuous functionality of ICT equipment, the Director ICT shall conduct regular maintenance of all ICT equipment. The Director ICT shall ensure that:

(i) For specialised equipment, only certified manufacturer's authorised Agents are allowed to provide Maintenance Services for ICT equipment in the Commission.

(ii) All ICT Hardware equipment is maintained at an optimal, operational and secure level.

(iii) All critical ICT Hardware have running Service Level Agreements.

ANNEX V: DATA AND INFORMATION SECURITY

ICT Security policy guidelines are aimed at safeguarding ICT Information Systems, Infrastructure, Information Assets, Computer Networks and Internet against any threats and to ensure confidentiality, integrity and availability of Commission's ecosystem and data therein. The following guidelines shall apply:

1. Logical Systems Security

(i) Users shall be issued with the level of access to ICT Systems required to perform their official duties after making application through the Head of their Service Areas.

(ii) Adequate systems security shall be put in place to ensure protection and integrity of ICT Systems.

(iii) There shall be an access control system maintained over all Information Assets according to their classification.

(iv) No User shall bypass any security control without the approval of the ICT Director.

(v) All Users of ICT Systems shall be responsible for the protection of information resources under their custody.

(vi) The Head of ICT Directorate shall, on behalf of the Commission:

(a) Be responsible for all Information Assets.

(b) Protect the ICT Systems and Services through effective control of security risks.

(c) Establish appropriate controls to limit access to ICT infrastructure, computer equipment, data and information.

(vii) A breach of security shall be handled in accordance with the TSC disciplinary procedures and/or the laws where necessary.

2. Unacceptable Information Systems Usage

The following Activities shall be strictly prohibited without any exceptions:

(i) Sharing of employee individual access privileges.

(ii) Usage of pirated Software on/in Commission's Information Systems.

(iii) Introduction of any malicious Software on/in Commission's Information Systems.

(iv) Any user action that disrupts or interferes with the normal Commission's Information Systems usage.

(v) Any password cracking, software spying, privilege escalation, unauthorised network port scanning and network reconnaissance, network and/or software penetration.

(vi) Installation or use of unauthorised Software or Information system.

(vii) Use of TSC Software or Information System outside the Commission without authority from the Commission Secretary.

(viii) Duplication or use of the Commission Software without authority from the Director ICT.

3. Password management

The following guidelines shall apply in defining the password strength and lifecycle specifications for all Users:

(i) Passwords shall be kept confidential and under no circumstance be shared.

(ii) The requirements for setting of passwords may vary from time to time depending on the best industry practice.

(iii) User name accounts or part of the User's full name will not be part of the password.

(iv) Passwords shall be composed of the following:

  (a) A minimum of eight (8) characters.

  (b) Alpha numeric, special characters, mixed characters' case and text.

  (c) The last three passwords should not be reused.

(v) Default Information Systems and Software Passwords shall be changed on first log in.

(vi) Passwords must be changed every 90 days.

(vii) Password must not be written down.

(viii) Passwords must be changed immediately if there is suspicion that the password confidentiality might be compromised and this reported to ICT Director for monitoring.

(ix) An in-house developed Information System shall use and support password encryption and user role segregation.

(x) In a case where a System has one administrator, the password escrow procedure shall ensure that an authorised person can access the Administrator's Account in case of an emergency.

(xi) When temporary access Accounts are required for Internal or External Audit, Software development, Installation or other reasons must be:

(a) Authorised.

(b) Created with specific expiry date and time.

(c) Deactivated and removed from the list of active Users upon expiry of the period.

(xii) All non-Commission Users must sign Non-Disclosure Agreement (NDA) before Account access is enabled.

(xiii) Passwords shall not be included in log on scripts or other automated log on processes.

(xiv) Password resets shall be requested only by the Owner of the Account except in exceptional cases as may be determined by the Director ICT.

(xv) Violation of the password guidelines may result to disciplinary action and /or legal action.

4. Cyber Security

The following guidelines shall apply to Cyber Security:

(i) The Commission shall have a Computer Incident Response Team (CIRT) whose mandate is to coordinate response and manage Cyber Security Incidents in the Commission and to collaborate with relevant actors on matters related to Cyber Security.

(ii) CIRT shall be the Cyber Security point of contact and is mandated with offering advice on Cyber Security matters in the Commission and coordinating response to Cyber Security Incidents in collaboration with relevant stakeholders as maybe approved by the Commission.

The CIRT shall:

(i) Be the risk owner for Cyber Security and will ensure that:

  (a) The internal ICT Systems are not a source of cyber risk.

  (b) Data exchange between the Systems complies with all security requirements and best practices.

  (c) Risk Register is maintained.

(ii) Ensure the implementation of the Information Security Management System (ISMS) Framework in the Commission.

(iii) Ensure that only authorised Users are allowed to access information and data on the Commission's network.

(iv) Provide leadership for the Governance of Cyber Security within the Commission.

(v) Co-ordinate and lead the rollout of periodic cross-cutting security awareness and training to all the employees of the Commission.

(vi) Co-ordinate a vulnerability assessment and penetration testing of all Systems and Infrastructure in the Commission on quarterly basis.

(vii) Ensure that all ICT equipment is installed with the appropriate active malware protection that is continuously updated.

(viii) Participate in the activation of the ICT BCP/DRP.

5. Bring Your Own Device (BYOD)

The Commission shall allow employees to bring their own devices in strict adherence to the following guidelines:

(i) The devices are approved and registered by the Director ICT.

(ii) The devices must have current TSC minimum Security Configurations and Software Specifications.

(iii) Devices must have no sensitive or confidential data, information and Information Systems stored or installed in them.

(iv) The Commission shall have the right to investigate and or audit such devices for any malicious activity, cybercrime or fraud without notification.

(v) The device is subject to all Commission's processes and configurations.

ANNEX VI: BUSINESS CONTINUITY PLAN

Guidelines for Disaster Recovery Plan

The ICT Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) provide a structured approach for responding to incidents that cause significant disruptions to critical ICT Services in the Commission.

The following guidelines shall apply:

(i) The Commission shall establish an ICT BCP/DRP as part of the Commission's Business Continuity.

(ii) DR Site shall be established and maintained as per the ICT BCP/DRP.

(iii) Director ICT shall ensure that business operations are restored or maintained in the required time in case of any disruption of service.

ANNEX VII: VIDEO/TELE CONFERENCE MEETINGS

The following guidelines shall apply during virtual meeting:

ICT shall recommend use of a secure robust System that can be centrally controlled. A System where only invited participants are allowed access shall be used.

The following guidelines shall be followed when attending and convening video/tele conference meetings:

(i) Commission Staff shall adhere to all processes and antiquate followed during physical meetings as much as practically possible.

(ii) Confidentiality – These meetings are official records of the Commission and confidentiality must be upheld.

(iii) The chair must make sure only those supposed to attend by taking a roll-call of the attendees before proceeding.

(iv) Preparation of meeting materials and protocols should be observed before presentation of documents including timely circulation and all necessary approvals.

(v) Members will go through the documents in good time to provide insightful input.

(vi) The Secretary of the Meeting will prepare writing materials for minutes/record taking in good time before a meeting starts.

(vii) Each participant shall ensure their technology works. Ensure availability of a good Internet Connectivity. Tools will have enough charge to avoid disruption.

(viii) Using Devices in the following priority; laptop, iPad/tablet and phone will be considered.

(ix) Participants will have one device as a backup where possible preferably a tablet or a phone.

(x) Participants shall join a video/teleconference meeting before it starts to have time to settle as necessary. This will help address any technological hiccups which will prevent disrupting an ongoing meeting.

(xi) Participants must prepare for such meetings professionally. Dress professionally even when dressed casually.

(xii) Participants will be aware of the surroundings, making sure the background is professional with similarity to an office setting as much as possible. Preferably plain walls, plain fabric, closed cabinets or similar background. Some conferencing facilities allows you to blur the background helping to address this problem.

(xiii) Participants will select a quiet place to avoid both internal and external disruption and noise.

(xiv) For a video conference, participants shall turn on camera and remain visible. Adjust the camera angles for the frame to fit appropriately. Camera shall remain on even when a participant leaves their seat.

(xv) Participants will make sure there is enough light where they conference from. Have the source of light in front with the darker side being behind. Participants will avoid sitting with the window behind them as the light will make one to be poorly visible.

(xvi) Participants will remain seated and present – using attentive body language, avoiding unnecessary leaving meetings too many times which create disruption.

(xvii) Participants will avoid fiddling with the Keyboard as Laptops have an inbuilt microphone which captures keystrokes making them disruptive to other members.

(xviii) Participants will mute the mic when not talking – This reduces interference from any surrounding noise and makes the contributing person be clearly heard.

(xix) Participants will project the voice to make everyone and especially the person taking minutes, record clearly without interrupting the meeting. The recording person will request for a pardon for any clarification.

(xx) Food is not allowed in meetings.

(xxi) Ear/Head Phones will be used where possible. This reduces possibility of eavesdropping into the meeting.

(xxii) Echo will be reduced by having only connecting one device at a time. Connecting two devices at ago in the same location causes feedback causing echo or other irritating sounds.

ANNEX VIII: CLOUD COMPUTING

These guidelines outline best practices and approval processes in relation to the use of cloud computing solutions that the Commission may decide to use to support data processing, sharing, storage and management.

Cloud computing refers to the delivery of computing services over a third-party proprietary System through Internet. These services involve Infrastructure Development Platforms and Software Applications. The Commission shall use internal cloud and government cloud where applicable with external cloud services being used with the express authority of the Commission Secretary.

The following shall be considered before considering any cloud computing solutions involving the Commission Data:

(i) Existing Government Policies and set Standards.

(ii) The type of Information and Data to be stored, their confidentiality and sensitivity.

(iii) The Country where the Service Provider or the Cloud Servers is located in line with the Government Policies.

(iv) The available risk mitigation measures and mitigation costs for External, Public and Hybrid Clouds, including through encryption of Data, segregation of Data, and appropriate contractual clauses.

(v) Whether storage of the Information and Data in question requires the agreement of, or at least consultation with, Staff and/or Third Parties.

(vi) Encryption mechanisms.

(vii) Physical segregation of the Commission's records on dedicated Servers.

(viii) Use of Cloud Services located in Countries with no intrusive Data Security Laws.

(ix) Development of special contractual terms and conditions to ensure the protection of the Commission's privileges and immunities.

(x) A legal contract Non-Disclosure Agreement (NDA).

(xi) Have appropriate Service Level Agreements with Vendors.

ANNEX IX: RISKS

Below are the Risks associated with the implementation of this Policy and their Mitigating Measures:

No.	TYPE OF RISK	MITIGATION MEASURE
1.	Poorly managed access to Systems and Information Assets could lead to Users having anonymity or excessive System privileges which could be abused to cause financial and/or reputational damage.	Proper use and authorisation of Systems using System Access Form.
2.	E-mail and other electronic communication platforms are not secure by design. The content transmitted could be sensitive in nature and unauthorised accessor negligence in using the Systems could lead to legal issues, reputational or financial damage.	Email and other electronic communication facilities provided by the Commission are for official business tools and information transmitted via these facilities will be considered business information, owned by the Commission. Personal emails shall not be used for Official Communication. Disclaimer at the bottom of emails will be added.
3.	Poorly configured and managed computing Assets could be a vehicle through which unauthorised access to Systems and Information Assets could be obtained.	All Commission equipment and those being used to transmit Commission information (BYOD) shall be configured as per the Commission Standards.

No.	TYPE OF RISK	MITIGATION MEASURE
4.	In-appropriate use of internet resources could have a negative impact on infrastructure capacity and availability. It could also expose internal resources when re-used credentials get compromised on external web platforms; and illegal activity by employees could expose Commission to legal and reputational risk.	Internet must be used as per the internet guidelines herein.
5.	There may be a risk of vulnerabilities or threats (internal and external) left unattended, which may be exploited by malicious Users or outside Attackers and may lead to the disruption of Commission Activities, Sensitive Information Disclosure, Fraud and potential reputational damage.	Regular Systems updates, Patches installation and Systems upgrades must be done as per the Systems guidelines herein.
6.	Unattended vulnerabilities or threats (internal and external) may be exploited by malicious Users or outside Attackers and may lead to the disruption of organisational Activities, Sensitive Information Disclosure, Fraud and potential reputational damage.	All reported/known vulnerabilities must be addressed immediately and recorded in the Service Desk System for rectification and automatic escalation.
7.	Incidents not logged, prioritised, authorised or contained could lead to a disruption of the Commission business Activities and damage its Information Assets. This could result in the extended unavailability of key Systems due to failure of addressing incidents.	All Incidents and User problems must be reported through logging them into the Service-Desk System by the users for follow-up and escalation.

No.	TYPE OF RISK	MITIGATION MEASURE
8.	Unauthorised, poorly tested and /or inadequately documented changes to IT Systems affecting the Commission's Information could cause disruption to production Systems, increase the risk of System and Information integrity being compromised or create vulnerabilities in Systems that can be abused by Parties with malicious intent.	All changes to IT Services must follow the Commission Change Management process by filling the Change Request forms. Systems must be properly tested in the test environment before being introduced to the production environment.
9.	A disaster, infrastructure failure or a cyber-attack could render business critical information un-available. If the business cannot restore the information from backups, it could lead to a breakdown of business processes.	ICT Business Continuity/Disaster Recovery Plan must be updated and tested with all relevant backups being regularly done as per this Policy.
10.	Physical unauthorised access to areas or infrastructure where sensitive equipment are kept or information is processed, could create opportunity to disrupt processing change or leak of sensitive Information.	ICT facilities must be designed with risk of data-loss in mind. Access to ICT Cabinets and Data Centres must be with an ICT Officer accompanying the Third Party who must sign the Data Centre Rules and Regulations.
11.	Poor selection of outsourcing services could create gaps in the security posture.	All outsourced Services and Locations must have agreements protecting the Commission's Data with serious legal implications on breach.
12	Risks may be incorrectly identified and communicated within the enterprise.	Appropriate risk responses need to be put in place for each incident reported.

ANNEX X: ICT EQUIPMENT ALLOCATION MATRIX

The Commission shall use the following guideline when issuing computing resources:

DESIGNATION	LAPTOP	DESKTOP	TABLET	PRINTER	CATEGORY
COMMISSIONERS	√	√	√	√	1
COMMISSION SECRETARY	√	√	√	√	1
DEPUTY COMMISSION SECRETARY	√	√	√	√	1
DIRECTORS	√		√	√	1
REGIONAL DIRECTORS	√		√	√	1
COUNTY DIRECTORS	√		√	√	2
DEPUTY DIRECTORS (HQ)	√		√	√	2
DEPUTY COUNTY DIRECTORS	√			√	2
SUB COUNTY DIRECTORS	√			√	2
DEPUTY SUB COUNTY DIRECTORS	√			√	2
ASSISTANT DEPUTY DIRECTORS		√		√	2
PRINCIPAL OFFICERS	√*	√		√**	2

DESIGNATION	LAPTOP	DESKTOP	TABLET	PRINTER	CATEGORY
SENIOR OFFICERS	√*	√		√**	2
PERSONAL ASSISTANTS (PA)	√		√	√**	2
OFFICERS I & BELOW		√		√**	3
SECRETARIES		√		√**	3

Category – Classification of the specification of Laptops and or Desktop Computers

1 – High End
2 – Standard
3 – Basic

√* Issuance of the laptop is subject to written justification that will be based on duties.

√** Shared Printer.

ANNEX XI: FORMS

TEACHERS SERVICE COMMISSION

Document No.:	TSC/ICT/FORM.1.0	Revision #:	0	Revision Date:	15 JUNE 2020
Title:	ICT EQUIPMENT ACKNOWLEDGEMENT FORM				
Employee Details					
NAME:				TSC NO:	
DESIGNATION:					
DIRECTORATE:				SECTION/UNIT:	
OFFICIAL EMAIL:	_				
SUPERVISOR:					
					Tick where applicable

ICT Equipment Details			YES	**NO**
TYPE:	Desktop Laptop Tablet	POWER CABLE(S)		
MAKE:		BAG		
MODEL:		MOUSE		
SPECIFICATIONS	OTHERS:	KEYBOARD		
SERIAL NO.		ASSET TAG NO.		
COLOR:		COMMENT(S):		

I acknowledge receiving the above equipment in good physical and working condition from the Teachers Service Commission. I am solely responsible for this device until it is returned to TSC ICT Directorate at the time of my separation from employment or on request from TSC through the Director of ICT. I will strictly use the equipment for official purpose only. By signing this document, I am accepting and agreeing to all TSC usage terms and policies.

Employee Signature:						Date:	_
Authorised issuing ICT Officer							
Name:			Sign:			Date:	

TEACHERS SERVICE COMMISSION

Document No.:	TSC/ICT/FORM.2.0	Revision No:	*0.1*	Revision Date:	15 JUNE 2020
TITLE:	ICT EQUIPMENT MOVEMENT FORM				
Employee Details					
NAME:				TSC NO:	
DESIGNATION:					
DIRECTORATE:				SECTION/UNIT:	
OFFICIAL EMAIL:				SUPERVISOR:	
MOVEMENT DETAILS					
FROM:		TO:			

REASON:					
ITEM	MAKE/ MODEL	SERIAL NO.	ASSET TAG NO.	QTY	
Employee Signature:				Date:	
Authorised issuing ICT Officer					
Name:		Sign:		Date:	

TEACHERS SERVICE COMMISSION

Document No.:	TSC/ICT/FORM.3.0	Revision No:	0.1	Revision Date:	15 JUNE 2020	
Title:	ICT SYSTEM ACCESS REQUEST FORM					
Employee Details						
REQUESTER NAME:				TSC NO:		
DIRECTORATE:				SECTION/UNIT:		
OFFICIAL EMAIL:				DESIGNATION:		
SIGNATURE:				DATE:		

System Requested for Access (tick as appropriate):

No	SYSTEM	√	CREATED BY	SIGN
	Active Directory			
	CRM			
	EDMS			
	Email			
	Help Desk			
	HRMIS			
	IDEA			
	IFMIS			
	Knowledge Base			
	Services			
	Teachers Online			
	Team-Mate			
	TPAD			
	T-Pay			
	Pydio			
	Other(Specify)			

Request Type: New user Change/Modify user Deactivate user

III. HOD Approval:

Systems Approved (How many) [_______] specify the systems (No 1,4,)……………..……………………………………………..

Approved by TSC/No: ………………. Name: ……………………………………………. Designation: ………………..………

Signature: ………………………………… Date: ………..………. Directorate/Division: …………………………………………….

IV. ICT Approval:

Approved by TSC/No: ………………. Name: ………………………………..……… Designation: …………..……………..……

Signature: ……………………..…………. Date: ……………..……. Specify the systems (e.g., a, b, c etc) ………………..….........

TEACHERS SERVICE COMMISSION

Document No.:	TSC / ICT / FORM.4.0	Revision No:	0.1	Revision Date:	15 JUNE 2020	
Title:	ICT SYSTEM CHANGE REQUEST FORM					
Employee Details						
REQUESTER NAME:			TSC NO:			
DIRECTORATE:			SECTION/UNIT:			
OFFICIAL EMAIL:			DESIGNATION:			
SIGNATURE:			DATE:			
Change Request						

Change Description/ Change Request Filename:							
System			Needed by (date):				
Description of the change:							
Reason for the change:							
Requestor Sign off:							
Process owner Approval:							
Change Impact Evaluation							
Change Type	Application		Database				
	Hardware		Procedures				
	Network		Security				
	Operating System/ Utilities		Schedule Outage				
Change Priority	Urgent/ High/ Medium/ Low		Change Impact	Minor/ Medium/ Major			
Environment(s) Impacted:							
Resource requirements: (personnel, HW, SW)							

Test Plan Description:					
Rollback Description:	.				
Change Approval or Rejection					
Change Request Status	Accepted:	Rejected:			
Comments:					
Change scheduled for (date):					
Implementation assigned to:					
Director ICT Sign off:					
Change Implementation					
Staging test results:					
Implementation test results:					
Date of Implementation					
Implementer Sign Off		Date:			

TEACHERS SERVICE COMMISSION

Document No.:	TSC/ICT/FORM.5.0	Revision No:	0.1	Revision Date:	15 JUNE 2020	
Title:	ICT LOST-DAMAGED EQUIPEMENT REPORTING FORM					
Employee Details						
REPORTER'S NAME:		TSC NO:				
DIRECTORATE:		SECTION/UNIT:				
OFFICIAL EMAIL:		DESIGNATION:				
SIGNATURE:		DATE:				

Type of Equipment:		Equipment status (must check one) √ Lost √ Damaged √ Stolen
Incident Date:		Needs Replacement?* √ Yes √ No
If stolen/Lost, Date reported to the Police:		

	If stolen/Lost, Police Report Reference No.:		
	Police Station reported:		
Description of Incident (write briefly what happened to the equipment)			
Equipment Information – check with ICT information			
Type/Make/Model:		Serial Number:	
Repair Cost Estimate		Approx. Equipment Cost:	
Equipment Specifications details:			
Designation	Name	Signature	Date
ADD SERVICE MGT:			

All stolen and lost equipment must be reported to the police. Submit this form to ICT after filing a police report.

Copy to send to Commission Secretary and SCMS

TEACHERS SERVICE COMMISSION

Document No.:	TSC/ICT/FORM.6.0	Revision No:	0.1	Revision Date:	15 JUNE 2020	
Title:	ICT DATA CENTRE ACCESS FORM					
Employee Details						
VISITOR'S FULL NAME:						
DATE:		TSC & ID No:				
ORGANISATION/SECTION:		MOBILE No:				
OFFICIAL EMAIL:		DESIGNATION:				
SIGNATURE IN:		TIME IN:				

Each individual will need to be pre-authorized by Director ICT by signing this form. This form along with the Data Centre ,Rules and Regulations must be signed by each individual and Deputy Director ICT Infrastructure and returned before Access is Authorised.

REASON FOR ACCESS

ICT Officer must collect each visitor's identification document before proceeding.

ACCOMPANYING ICT OFFICER:			
NAME:		SIGNATURE:	
TSC NO:		DATE:	

APPROVED BY DIRECTOR ICT			
NAME:		SIGNATURE:	
TSC NO:		DATE:	
VISITORS' SIGNATURE OUT:			TIME OUT:

TEACHERS SERVICE DATA CENTRE RULES AND REGULATIONS

1. All TSC employees, Service Providers and their representatives, employees, contractors, agents, invitees, and users of TSCs' facilities and all TSC contractors, vendors, invitees, or agents ("Authorised Persons") are subject to these Rules and Regulations in connection with their use or access to the TSC Data Centre or ICT Cabinets.

2. All equipment installation activities must be pre-approved by TSC. Any Authorised Service Provider Person installing any type of equipment into their equipment within the Data Centre must first check in with Deputy Director ICT – Network and Infrastructure and provide the necessary information about the equipment and the installation prior to commencing any installation activities.

3. All power and power distribution must be provided and installed by TSC personnel. In the event that an Authorised Person wishes to provide their own power distribution, TSC electrician must be present during the installation.

4. Connecting one power strip into another, also referred to as 'Daisy-Chaining' is not permitted under any circumstances. Daisy-Chaining not only presents a fire-hazard but also presents the potential to overload a power circuit resulting in a loss of power to a power strip, receptacle or complete bus.

5. TSC expects all Authorised Persons to adhere to the 80/20 rule regarding power consumption. This requires that typical power usage is not to exceed 80% of total power available per power circuit.

6. An Authorised Person is not permitted to and shall not approach, handle, use, inspect or examine any equipment, cabinets, cage space, local deployment workstation or floor space, other than their own or one which they are supposed to be working on.

7. An Authorised Person's access to or use of the Data Centre and the TSC building shall at all times comply with the rules and regulations promulgated by TSC from time to time.

8. An Authorised Person is not permitted to and shall not at any time disclose the information about any TSC equipment.

9. The TSC building shall be kept neat and orderly at all times. Authorised Persons shall remove all of their trash and debris upon departure from the building. TSC shall have the right to remove and discard any trash and debris left in the TSC building in violation of the foregoing, and to charge the Authorised Person for such trash removal.

10. Flammable items (i.e.; cardboard and paper) are not to be stored within any collocated space throughout the datacentre. These items filch humidity from the air, present a fire hazard and introduce dust contaminants into the air.

11. At the conclusion of any work in the Data Centre, the Authorised Persons shall ensure all cables are routed and dressed neatly in cabinets and all doors are closed and locked and the equipment or area is left in a closed, orderly, and secure manner. The Authorised Persons may bring into the Data Centre tools and portable test equipment, approved by TSC, provided that the Authorised Persons are responsible for and remove or secure the same upon their departure from the Data Centre. Any Authorised Person utilising the Local Deployment Workstations will be responsible for securing all of their own equipment, documents and supplies.

12. Any and all equipment, including Customer Equipment, operated within a Data Centre must be configured and operate at all times in compliance with the applicable manufacturer's specifications, including, without limitation, any specifications as to power consumption and/or clearance requirements.

13. In the event that a hardware failure of any equipment results in an audible alarm being emitted from the equipment, the Service Provider will be asked to resolve such alarm within 14 days of being notified of its existence. Alarms of this type are disruptive to other Authorised Persons accessing the data centre facilities and also impair the ability of Technical Operations staff to identify other audible alarms on other equipment or data centre infrastructure during facility walkthroughs.

14. No sign, advertisement, notice or object shall be displayed by a Service Provider, Contractor, Supplier or Visitor in or on the exterior of the Data Centre walls, doors, ceilings, racks, cabinets or cages without TSC's prior approval.

15. No Authorised Person shall bring into or keep upon the Data Centre premises any hazardous, combustible, explosive, or otherwise dangerous fluid, chemical or substance at any time.

16. No acids, vapors or other materials shall be discharged or permitted to be discharged into the waste lines, vents or flues of the Data Centre.

17. Authorised Persons may not bring or use any of the following in the Data Centre; Tobacco Products, Explosives, Weapons, Chemicals, Illegal drugs, Electro-magnetic devices, Radioactive materials, Photographic or recording equipment of any kind.

18. Food and beverages may be allowed in the office areas of the Data Centre with TSC's prior permission. No food and/or drink will be allowed under any

circumstances in any of the data centre space, ICT cabinets or in the main distribution frames. Any breach of this Policy will result in immediate loss of access privileges.

19. TSC reserves the right to inspect all objects to be brought into or taken out of the Data Centre and to exclude from the Data Centre all objects which violate any of these Rules and Regulations. TSC may require any person entering or leaving the Data Centre with any package to document the contents of the package.

20. All provided connections to and from Service Provider Equipment will be clearly labelled. It is imperative that these labels remain intact so that TSC personnel can easily identify and troubleshoot any of the services it provides.

21. Periodically, TSC will conduct routine, non-emergency scheduled maintenance of its Data Centre and Services. TSC shall notify Service Providers a minimum of two business days in advance of said maintenance window.

ACCESS CONTROL

1. Only those individuals specifically identified by an authorised employee of the Service Provider or Contractor may access the Data Centre ("Permitted Individuals").

2. All Authorised Persons are required to log in upon entry, provide a National ID or other government issued photo identification and are then issued their TSC badge for access into and throughout the Data Centre. TSC will retain the Authorized Person's identification in exchange for the badge while the Authorised Person is in the Data Centre. The badge must be returned before the Authorised Person leaves the Data Centre.

3. "Tailgating" is prohibited. Tailgating is defined as the act of following a badged individual through access-controlled doors without following proper registration and authorisation procedures. TSC considers it the responsibility of badge carriers to ensure unauthorised individuals do not follow them through access-controlled doors.

4. Authorised Persons shall not access any portion of the Data Centre (except those they are working on), including without limitation, the building roof, electrical or communications closets, the Data Centre ceiling or floor, without prior consent from TSC.

5. All entries into the Data Center shall be accompanied by a TSC ICT personnel.

CONDUCT GUIDELINES

1. Authorised Persons may not misuse or abuse any TSC property or equipment.
2. Authorised Persons may not verbally or physically harass, threaten, intimidate, or abuse any individual within the Data Centre or while on TSC property, including without limitation, employees, agents, or invitees of TSC or other visitors. Abusive and threatening or offensive behaviour by any visitor will not be tolerated.
3. Authorised Persons may not engage or assist in any activity that violates the law or aids in criminal activity while in the Data Centre or on TSC property or in connection with the Services.
4. TSC may refuse entry to, or require the immediate departure of, any individual who (i) is disorderly, (ii) fails to comply with these Rules and Regulations, or (iii) fails to comply with any of TSC's other policies, procedures and requirements after being advised of them.

MODIFICATION OF RULES AND REGULATIONS

TSC reserves the right to change these Rules and Regulations at any time without notice of any such change.

By signing below, you agree to adhere to the TSC Data Center Access Rules and Regulations.

Authorised Employee's or Contractor's Name (please print):	
Signature:	**Date:**
DD ICT Infrastructure Name (Please Print):	DD ICT Infrastructure Signature: