MITOOMA DISTRICT LOCAL GOVERNMENT

INFORMATION AND COMMUNICATIONS TECHNOLOGY POLICY

VERSION1.0

(January, 2020)

FOREWORD

Mitooma district local government has embraced developments in ICT. In a bid to meet the National ICT policy2014 objectives, the district has developed District ICT Policy guidelines. The objective of this policy is to guide the district move towards realizing the district objectives in particular and the national Objectives in General.

The District recognizes the role of ICT in planning, budgeting, programme implementation, monitoring and evaluation of performance. As such, efforts have been made to equip and support the use and development of ICT initiatives in the district. These initiatives include:

Acquisition of ICT equipment such as Desktop Computers, Laptops, Printers, Photocopiers, Projectors, UPSs and other peripherals, Connection of internet services through a Local Area Network (LAN) and wireless network, Connection of telephone services using PBXs to improve internal communication, Design and implementation of District website and Recruitment of IT staff to manage ICT affairs.

To harness benefits from these initiatives, there is need for clear policies and operational guidelines for use and application of ICT resources. This guideline focuses on five (5) key areas in the ICT Policy and how they will be executed at an operational, middle-line and top management levels. Reference shall always be made to the relevant policy as pertains to its use, application and consequence. The policies referred to here are:

Acceptable Use of Information and Communications Technology Resources, Data Security, Physical Information and Communications Technology Security, Disposal of Information and Communication Technology Equipment and Web Content Publishing in the entire IMS.

Key operational activities related to each policy have been identified and guidance is hereby made to support their implementation to enable the district realize full benefits of using ICT as an important resource for social – economic development.

Tumukurate Silvaster
AG. CHAIRMAN MITOOMA DISTRICT LOCAL GOVERNMENT

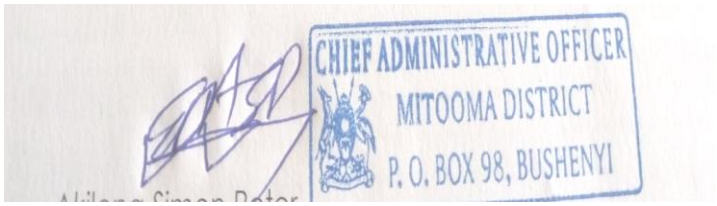
ACKNOWLEDGEMENT

This District Information and Communications Technology (ICT) Policy was developed in consultations with all sector and departmental heads, reviewed through Technical Planning Committee and planning unit.

I'm grateful to those persons who in one way or the other contributed to the production of this policy. The Quality of the policy reflects the commitment and interest members have attached to this document.

I wish to call upon all members of staff to put this policy into use to realize the intended objectives to promote socio – economic development in the district.

Special thanks go to the District Planning Unit for their role in the formulation of the policy.



AKILENG SIMONPETER
CHIEF ADMINISTRATIVE OFFICER/ MITOOMA DISTRICT

Contents

ABBREVIATIONS

CAO ------- Chief Administrative Officer

E- WM ---- Electronic Waste Management

ICT ---------Information Communications Technology

IT----------Information Technology

LAN --------Local Area Network

MIS --------Management Information System

NAC -------Network Access Control

NEMA ----National Environmental Management Authority

PBX -------Private Branch Exchange

SLA -------Service Level Agreement

UPS -------Uninterruptible Power Supply

PHRO-----Principal Human Resource Officer

DPO-------Principal Production Officer

LLG-------Lower Local Governments

SOP-------Standard Operating procedures

VPN------ Virtual Private Network

M&E-------Monitoring and Evaluation

WWW-----World Wide Web

PPDA------Public Procurement and Disposal of Public Assets Act

PDU--------District Procurement and Disposal Unit

GLOSSARY OF TERMS

Consumer: An Organization or individual that uses electrical and electronic equipment and then discards it as waste after the equipment has reached its end – of –life. Note that the end - of - life for a consumer, may feed into the second – hand market directly or through refurbishers.

User: Any individual who has access to our information systems for the purpose of performing work. Users consist of, but are not limited to: employees, Councilors, third parties etc.

End – of life: Refers to the end of the useful life of equipment in a particular environment. The equipment may then be passed onto the second – hand market. This is distinct from lifespan, which describes the total functional life of the equipment.

Electronic waste (e-waste): refers to electrical or electronic equipment which is waste - including all components, subassemblies and consumables, which are part of the product at the time of discarding. It includes computers and entertainment electronics consisting of valuable as well as harmful and toxic components.

Distributors/retailers: Include all bodies selling equipment to the end – consumer, including donated computers.

Recyclers: Organizations dismantling, separating fractions, and recovering into the second-hard market.

Refurbishers: Refurbishing extends the functional life of equipment. Refurbishers include the repair and service centers. They often feed into the second- hard market.

Importers / assemblers: Importers and / or assemblers of branded and non- branded electrical and electronic equipment.

Collectors: Formal or non – formal bodies that collect e – waste. This may involve procuring bonded computers from government, parastatals and private organizations.

Server: A computer or computer program that manages access to a centralized resource or service in a network.

Remote Access: The ability to obtain right of use to Mitooma district ICT system from a location or via a system not owned by the district.

Firewall: A system access control device that acts as a barrier between two or more segments of a computer network to protect internal networks from unauthorized users or processes of other networks.

ICT Infrastructure: All ICT hardware and software systems.

Virus: A dangerous piece of programming-code that attacks computer and network systems with the aim of causing them to malfunction. This includes; spyware and malware.

IT Steering Committee: The sub-committee that gives general oversight to IT related issues.

Wireless Network: A network utilizing radio waves to transmit data as opposed to physical wired connections. Example of a wireless network is Wi-Fi.

World Wide Web (www): A hypertext-based distributed information system for linking databases, servers, and pages of information available across the Internet.

Internet: A world wide web or computer network through which you can send a letter, chat to people electronically or search for information on almost any subject you can think of.

1. INTRODUCTION

This document entails the policies and guidelines that apply to the ICT department Mitooma District Local Government. These policies and guidelines are critical for providing assurance to government, funders, regulators, and auditors that Mitooma district takes seriously the confidentiality, integrity and availability of data placed in its care. They are therefore designed to carefully control the growth and operation of the ICT function and its cost, consistent with the district goals and objectives. Due to the nature of her structure, considering visitors, employees, volunteers, students, vendors among others, the information at different levels has to be secured and protected from any kind of threats. It is therefore imperative that they are clearly read, understood, and implemented by all users of the district's ICT facilities in a manner that will result into efficient and cost-effective operation of the ICT facilities.

1.1. OBJECTIVES

1.1.1. Main Objective

The main objective of the ICT policy is to provide for the centralized effective governance of all ICT related matters within the district in a rationalized and harmonized manner.

1.1.1. Specific Objectives

The specific objectives of the ICT Policy are:

a. To promote the usage of ICTs in conducting business of the district LG administration
b. To define management roles and governance structures to guide ICT functions at the District LG Administration
c. To provide guidelines and procedures for planning, designing, procurement, installation, usage, maintenance and support to all user units
d. To provide guidelines to enhance access to ICT services and support
e. To put in place guidelines and procedures for security for ICT facilities and services

1.1.2. Legal Framework

The district ICT policy shall be in line with the following laws and policies:

a. The Constitution of the Republic of Uganda (1995).
b. The National ICT Policy (2014)
c. The Communications Act (2013)
d. The Computer Misuse Act(2011)
e. The Electronic Transactions Act(2011)
f. The Access to Information Act (2005)
g. The Uganda Human Rights Act, Cap.24

h. The National Information Technology Authority Act, 2009
i. The Uganda Communication Regulatory Authority Act, 2012

2. POLICIES AND GUIDELINES

2.1. POLICY: Acceptable Use of Information and Communications Technology Resources

2.1.1. PURPOSE

Mitooma district has invested in information and communication technology infrastructure in an effort to improve its administrative and operational functions. The district considers information and communications technology (ICT) resources to be a valuable asset whose use must be managed to ensure their integrity, security and availability for lawful administrative and operational purposes.

While the district seeks to promote and facilitate the use of ICT resources, such use must be done responsibly and must respect the rights of other users. This document is provided to give guidelines to users of information technology resources, without compromising on the ethics and conduct of staff in the day to day administration of office operations.

2.1.2. SCOPE

This acceptable use policy applies to all users of the District headquarter offices, Sub County and Town Council ICT resources. The resources referred to in this policy include but are not limited to the following: -

1. The network and related network services
2. District, Sub County and Town Council Computers and related peripherals (Desktop Computers, Laptops, Printers, etc.)
3. Management Information Systems
4. The Database systems
5. Any other system that may be installed to provide a service to the District, Sub County or Town Council.

Users of ICT resources in this case are defined as any individual who uses or attempts to use the ICT resources described herein, and may include District, Sub County or Town Council Staff, Political Leaders, Intern students and some individuals granted permission to use resources. The definition also covers any authorized individual who connects, attempts to connect to the District network whether from within the District or from remote locations.

2.1.3. USER RESPONSIBILITIES

Mitooma District ICT resources are provided primarily to facilitate a person's work as an employee, Political leader, Researcher or any other role within the District structures. Use of ICT resources for other purposes, such as personal or recreational use is a privilege, which can be withdrawn.

In all cases, users are obliged to use resources responsibly to ensure their Security and availability to other users. Acceptable use of the District ICT resources may include:

i. Use for official business, including preparation of reports, Minutes, Presentations etc;
ii. Use for communication purposes;
iii. Use for Data entry, Analysis and storage.
iv. Use for Data management

Unacceptable use of the ICT resources may include but are not limited to;

i. Attempts to break into or damage computer systems within the network or in other connected networks or individually at the district, sub county or town Council
ii. Attempt to access computers for which the individual is not authorized.
iii. Unauthorized access to another user's files/ IP address.
iv. Attempting to circumvent Network Access Control, including by-passing proxies and firewalls.
v. Monitoring or interception of network traffic without permission.
vi. Probing for security weakness of systems by methods such as port scanning, password cracking, without permission.
vii. Unauthorized extension or retransmission of network traffic including the installation of unauthorized wireless access points, routers or switches.
viii. Unauthorized reselling of network and information Management systems services.
ix. Unauthorized modification of District or/and sub county/ town Council data.
x. Unauthorized download, installation or running of programmes or utilities that may flood the network causing denial of services to other users.
xi. Sharing of network access credential with third parties for purposes of defeating network authentication.
xii. Using the network to break into other networks.
xiii. Creation, retention, downloading or transmission of any offensive, obscene or in decent images or data or any data capable of being resolved into obscene or in decent image or material.
xiv. Creation, retention, or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety.
xv. Intellectual property rights infringement, including copy right, trademarks, patent, design and moral rights.
xvi. Sending electronic mail that purports to come from an individual other than the person actually sending the message using, for example a forged address.
xvii. Using the resources for unsolicited advertising or transmission of electronic mail with intent to defraud often referred to as "Spamming".
xviii. Deliberate unauthorized access to networked resources, local or remote.
xix. Actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software.
xx. Downloading, installation and use of unlicensed software on the district network and Computers.

xxi. Deliberate activities that may result to one of the following;

- Wasting of support staff time in support systems
- Corrupting or destroying other users' data
- Violating the privacy of other users
- Denying services to other users

2.2. POLICY: Information and Network Security

All end-user personal computers and workstations must have virus protection software installed. The antivirus solutions must be routinely updated and deployed from a centralized location. The antivirus agents must be remotely deployed to scan all hosts on the network. All users shall be required to pay attention to attachments that come from unknown sources as they may contain virus(es) that can affect the entire network.

All network devices including any data traffic shall be monitored using firewalls in order to detect and respond to faults immediately and ensure network security. Modification of any network connections shall only be done by ICT support staff. Any component of the ICT system suspected of transmitting dangerous traffic shall be disconnected from the Local Area Network (LAN) immediately.

All computers used in the district will be protected against dynamic content based threats like viruses, Trojan horses, worms, spyware, phishing and application vulnerability exploits. The district will also implement better usage and follow up regularly on the email server and work on the Network security to avoid network based threats such as spoofing, protocol analyzers, and denial of service.

All internally and externally bound links to the network shall be compliant with standards relating to network security and access controls including but not limited to filtering, logging, Virtual Private Network (VPN), two-factor authentication, Wi-Fi passwords and encryption.

2.3. POLICY: Data Security

2.3.1. PURPOSE

The purpose of this policy is to identify and disseminate the District's framework and principles that guide Organizational actions and operations in generating and sharing confidential information. Information assets in all forms and throughout their life cycle will be protected through information management policies and actions that meet applicable regulations, laws and contractual requirements to support the District's mission, Vision, main Goal and District Council Objectives including all sub counties and town councils.

2.3.2. SCOPE

This policy applies to all staff, intern students, Vendors, Volunteers, Contractors or Other affiliates of Mitooma District with access to confidential institutional Information. The scope of the information includes all electronic data elements, which belong to the District and all its lower local government structures that satisfy one or more of the following criteria:

- The data is relevant to planning, managing, operating, or auditing a major administrative function of the District
- The data is referenced or required for use by more than one department
- The data is included in an official District administrative report
- The data is used to derive a data element that meets these criteria

2.3.3. USER RESPONSIBILITY

The electronic data of the District either reside on central district system server or on desktops, laptops and other mobile devices belonging to individual users. In either circumstance, users must be aware of policy issues governing their protection and access.

The following policy statements thus apply:

All District data as specified in section 4.1 shall be stored on centrally maintained server while all sub county data shall be maintained by each sub county individually on their local computers with backup files kept with the district. In the event that such data is stored on user desktops, laptops and other mobile devices, it is the responsibility of the user to ensure its security, confidentiality and integrity in respect to this policy such as regular backup, password protection etc.

All access to data stored in central administrative databases must be through standard interfaces provided for by the various information systems (if any)

Requests for Access to all administrative data and the central systems in general must be authorized by the relevant Data Owner (i.e. CAO, Planner, Finance Officer, PHRO, DPO and all other Sector Heads respectively. The granting of access is then effected by the Officer responsible for managing ICT resources.

In the event that confidential information is protected by technical security mechanisms (physical or electronic) using safes, passwords etc. and these mechanisms fail or are absent, users are obliged to protect confidential information from public access. Lack of security, such as making private information, public

2.3.4. TECHNICAL STAFF RESPONSIBILITY

The responsibility for protecting all important data stored in central district systems (servers, database, network storage etc.) is the mandate of the ICT Officer with the guidance of the Chief Administrative Officer. The guiding policies for this role are as stipulated in the following Section.

All District data residing on the central network storage must be backed up on a regular basis. Frequency of backup is determined by the frequency with which the data changes and the effort required to recreate the information if lost. Standards apply to the backup of data from all District systems. All sub county data shall be backed up and a copy of data of each sub county kept at the district headquarters. All restore procedures must be properly documented and tested on a regular basis, at least annually. Backup media must be stored in a secure or an off – site

location and retrievable within 24 hours, 365 days a year. Off – site is synonymous with "out of the building''. The off- site storage location must provide evidence of adequate fire and theft protection and environmental controls. A site visit should be undertaken on an annual basis and where appropriate, a formal Service Level Agreement (SLA) must exist with the off- site storage provider.

Backup and recovery procedures must be developed and maintained for all administrative computing systems and data. The following requirements must be met:

- Provisions for regular backup of data residing on the system.
- Storage of backup media at a location remote from the processing center.
- Approved Disaster Recovery plan written and implemented to cover situations in which hardware and / or software cannot run in its normal environment.

Data owners in their role as custodians of district data are responsible for defining and documenting the length of time data must be retained. The retention period, legal requirements, responsible parties, and source of legal requirement should be specified. The ICT Officer will be responsible for ensuring that these requirements are adhered to.

If any Database management software is used for administrative application development, it should meet the following features:

- Ability to designate the database "private" or "public"
- Access capabilities which can be restricted at the table and field levels
- Access capabilities which can be restricted based on user, time of day, day of week
- Audit trails/ journals which record important activity
- Control checkpoints

For any software purchased or redeveloped, pre-software testing will be carried out to ensure that it meets the accuracy, validity and reliability standards required by the user, and will have sufficient documentation on structure, function and integration with other software used by the group. An up to date software inventory, approval of installation and use of new software will be maintained and managed by the systems administrator using the ICT form (Approval of installation and use of new Software).

2.4. POLICY: Physical Information & Communications Technology Security

2.4.1. PURPOSE

The purpose of this document is to identify Mitooma District frame work and principles that protect institutional actions and operations in responsible use of its ICT resources.

2.4.2. PREAMBLE

The District has made strong efforts to invest in establishing ICT infrastructure both at the headquarters and lower local governments. The Value of ICT investment accrues when users demonstrate responsible use of the infrastructure and it starts to gradually break down much

faster than its useful life span. Security in this context refers to measures that shall be taken to ensure that physical availability of all ICT resources is not compromised in any way. All departments and LLGs shall be required to define an "owner" of each piece (e.g. a computer, laptop, printer in an office) or group (say in a computer lab or server room) of equipment and that individual shall take the responsibility of ensuring its security.

All backbone equipment shall be the responsibility of the ICT responsible Officer.

2.4.3. SCOPE

The Policy applies to all staff, trainees, students, vendors, volunteers, interns, contractors or other affiliates of Mitooma District with access to the District and LLGs ICT resources.

2.4.4. POLICY STATEMENTS

Only authorized staff and political leaders are permitted to open and use computers or related systems. Other staff, Intern students, Visitors shall access with permission/ authorization from a responsible Officer.

No computer equipment and other accessories shall be carried out of the Office sunless the responsible Officer has given explicit permission. As such Equipment movement forms shall be put in place to facilitate this measure.

The ICT Officer shall maintain an asset register where such moves are monitored and tracked. A logical and systematic naming convention shall be adopted uniquely to identify all ICT equipment and where applicable, shall match the corresponding asset tag. An up-to-date inventory of all ICT equipment shall be maintained by the ICT department using an ICT equipment inventory form.

In the event that the allocated ICT equipment is lost or stolen, the user shall immediately report to the ICT officer and/or Security personnel and other relevant authorities.

There shall be adequate damage prevention systems such as fire suppression using smoke, fire detecting devices and fire extinguishers installed/placed in all sensitive ICT infrastructure areas. And in case of fire outbreak signaled by a fire alarm, all building occupants are to vacate it to the assembling point till the problem is resolved.

Authority to access sensitive ICT infrastructure such as server rooms, communication rooms, etc., shall be granted by the ICT Officer, Head of Planning Unit or the CAO and a record maintained through ICT form (Approval to access ICT systems).

2.5. POLICY: Disposal of Information and Communication Technology Equipment (Electronic – Waste management)

2.5.1. BRIEF DESCRIPTION

Information and Communication Technology equipment have an average useful life span of four years. After the lapse of its useful life, this equipment is considered to be obsolete. Obsolete equipment should be disposed off in an environmentally friendly manner.

The District as one of the organizations with ICT equipment in this Country is obliged bylaw to implement a sustainable environmentally friendly electronic waste disposal policy. All information and Technology equipment have an average life span of 4 (four) years because new computer technology evolves almost every 6 months. After 4 years this equipment gets depreciated and obsolete equipment may continue to function during its salvage value for a while before it outlives its usefulness. Wear and tear of obsolete equipment can be hastened by the conditions which the equipment is subjected to, like power stability, dust, end – user handling and moisture.

ICT equipment that is due to outlive its useful life continues to erode the quality of end –user output through regular breakdown until it completely degenerates. ICT equipment, like computers, may be salvaged to assemble functional equipment like personal computer, which may then be re- deployed for use, donated or sold.

2.5.2. POLICY STATEMENT

The ICT Officer shall be mandated with the monitoring, acquisition and management of disposal of all ICT equipment in liaison with the Procurement Unit and user unit. Will develop guidelines and make recommendations for useful life spans of different equipment, salvaging, storing, donating, trashing and disposing of obsolete information technology products.

The District will maintain partnership with relevant policy and disposal organizations like the National Environmental Authority (NEMA), Electronic waste collectors, refurbishes, ICT Importers and assemblers, distributors and retailers.

Any equipment declared unusable will be documented and approval will be sought from the ICT steering committee to have it disposed off, following the set disposal procedures which include erasing and resetting the devices. All District user departments and LLGs shall be required to avail obsolete ICT equipment to the responsible Officer for disposal.

2.5.3. PROCEDURE

The ICT Officer will physically or electronically track the physical locations and status of all core ICT hardware components of the District and LLGs from the assets register manually or electronically from the database.

Any user department wishing to dispose of obsolete ICT equipment shall contact the responsible Officer who will evaluate the hardware and determine the appropriate course of action, according to set guidelines.

ICT equipment may be disposed of in the following ways:

Recoveries from offices – Equipment identified for disposal during the annual information system inventory taking exercise may be salvaged and re- assembled. The refurbished computers may be placed in a pool of computers of allocation to new staff or staff in need of computers may be placed in some common rooms for general computing needs (Internet browsing, document production etc.).

Hardware sale – Obsolete hardware may be sold at salvage value. The District Finance Department may assess the hardware and advise on the appropriate market price for the hardware sale. The Procurement unit may advise on the procedures of hardware sales. All hardware for sale should be presented for technical inspection to ensure that it does not contain any licensed software or council information. The responsible Officer will delete all information on the hardware and replace existing software with free equivalents, before the technical inspection.

Hardware donations – Obsolete hardware for donation to community outside the District should follow guidelines laid down by the national ICT policy on deployment of used technology equipment and environmental conservation. All hardware for donation should be presented for technical inspection to ensure that it does not contain any licensed software or district information. The responsible Officer will delete all information on the hardware and replace existing software with free equivalents, before they are donated.

Hardware destruction – Obsolete hardware that may neither be salvaged, nor sold nor donated may be destroyed. An inventory of hardware that has been destroyed or is due for destruction must be maintained. All hardware that has been destroyed or is due for destruction must be maintained. All hardware destruction should be done in accordance with available hardware destruction statutes or legal requirements.

2.6. POLICY: Information and Communication Technology Procurement

Procurement of all ICT equipment and services shall be in conformity with the overall District procurement of goods and services standard as aligned to the Public Procurement and Disposal of Public Assets Act (PPDA).

In addition, the procurement shall comply with the guidelines and standards for acquisition of Information Technology hardware and software for Government Ministries, Departments, Agencies (MDAs) and local government (LG) Administrations. These guidelines provide a framework for the procurement of ICT equipment and services with emphasis on standardization of ICT assets, transparency, timely delivery, quality assurance, and value for money as well as compatibility with existing infrastructure and services. District Procurement and Disposal Unit

(PDU)shall manage all procurement or disposal activities within the district in line with the PPDA (Section 31 & 32).The Information Technology Officer shall provide technical support and guidance on all matters of procurement, utilization and maintenance of ICT hardware and software to the District.

2.7. POLICY: Web Content Publishing

2.7.1. PURPOSE

Mitooma District has worked hard to provide social services to its people to promote Socio-economic development. To maintain and build upon that reputation, we must concern ourselves with the image we project.

The Web Publishing Policy exists to facilitate usability and consistency and to promote a Standardized District with a Website that correlates directly with sectors, departments, LLGs and the public.

A uniform and professional Communication standard will help us achieve this end. This policy will be supplemented by the Web Standards Guide, which contains up – to – date style guidelines, accessibility guidelines, and other information that may change on aperiodic basis.

2.7.2. SCOPE

Any Web document that represents Mitooma District Local Government is expected to follow this policy and the Web Standards supplement and should be in compliance within a reasonable amount of time after any change.

2.7.3. POLICY STATEMENT

The District considers web publishing to be a key strategic resource for communication, planning, research, marketing, and administration. The appropriate use of this technology by the District community is encouraged. However, the District reserves its right to define and limit the terms of use of its website.

District resources may be used to create and publish web pages where the purpose and effect of the published information is in support of the District's mission. This means that the content of web pages hosted on District resources must relate to the official activities and functions of the District or relate to the official role of members of the District community.

2.8. WEB CONTENT PUBLISHING REQUIREMENTS

2.8.1. ACCESSIBILITY

Mitooma District website must strive to adhere to the Web Content Accessibility Guidelines of the World Wide Web (www) Consortium. These guidelines are required of all Websites, regardless of any written exception approvals or other restrictions in the Web standards and Guidelines.

2.8.2. REDUNDANCY

Do not repeat static information maintained elsewhere by the District.

2.8.3. CONTENT VALIDITY

i. Mitooma District Local Government controlled site must be registered under the mitooma.go.ug. Domain
ii. Content must be up – to date and follow all sections of this policy and its Supplements, as well as national law and codes
iii. The ICT Officer shall have the mandate to manage and maintain the website in an acceptable state and shall be updated from time to time in collaboration with the district service providers.

2.8.4. COPYRIGHT

a. All District Web pages should follow copyright laws
b. Publishers must have permission from any copyright holder to use text, Photos, graphics, sounds, or movies to which Mitooma District does not hold copyrights

2.9. THE CROSS CUTTING POLICY AREAS

These include ICT infrastructure, Private sector participation, National ICT Standards, Information Security, Human Resource Development, Research and Development, Universal Access, ICT in Governance, Mainstreaming Women, Youth and PWDs Issues, ICT Promotion and Awareness.

The following strategies are to be lined up:

a) Optimize the connectivity to the undersea fiber optic cables in the district.
b) Encourage participation of the private sector in ICT infrastructure development.
c) Put in place mechanisms for quality assurance in infrastructure development.
d) Encourage Internet Service Providers (ISPs) to provide access to the network based services to even the most remote/hard to reach locations in the district like Kiyanga Subcounty.
e) Implement ICT Security awareness programmes amongst institutional and individual users.
f) Implement systems that will help in the detection, prevention and timely response to threats relating to ICT crimes and misuse.
g) Encourage ICT companies in the district to play a significant role in ICT education through internship and industrial training schemes
h) Ensure equal opportunity in basic ICT training at all levels taking into consideration special interest groups namely; Women, Youth and PWDs.
i) Attract local initiatives aimed at promoting investments in Community Radio stations, Internet, computerization, and ICT literacy training.
j) Act as change agents for information dissemination on the role and benefits of ICTs in socio- economic development, especially in communities.

3. ICT POLICY IMPLEMENTATION

3.1. POLICY STATEMENT

The ICT officer shall be responsible for implementation of this ICT policy and guidelines. All users of Mitooma district ICT systems and services shall be required to read, understand and comply with this policy and guidelines. The Policy owners shall closely monitor and enforce compliance.

3.2. SENSITIZATION OF THE POLICY

This ICT policy will be sensitized to all existing users through a workshop. The policies will be sensitized to all new staff during their orientation period immediately after reporting for duty. They will also be distributed to all Mitooma district staff, displayed on key notice boards and placed on the shared drive on the network for easy access at all times.

3.3. MONITORING AND EVALUATION

All ICT systems, as with all other assets, are the property of the District. The District Administration, therefore, reserves the right to monitor these systems to ensure compliance with this policy. The monitoring of the ICT system activities shall be carried out in a manner that respects the rights and legitimate interests of those concerned. Users of the district's ICT systems should be aware that their activities can be monitored and they should not have any expectation of privacy. In order to maintain their privacy, users of the district's ICT resources should avoid storing information on these systems that they consider private. By using the District's ICT systems, users expressly consent to the monitoring of all their activities within the District's ICT systems.

3.4. POLICY CONTINUITY

Policies and guidelines are dynamic and therefore, they shall be routinely reviewed and modified/updated by the ICT steering committee, as need arises, to reflect the district's emerging ICT requirements and changes in the environment and the expectations of members of the Mitooma district local government.

3.5. EMPLOYEE'S STATEMENT OF UNDERSTANDING

All users of Mitooma district local government shall be required to receive, read and understand this set of ICT policies and guidelines. All users shall undertake to comply with the consequences of violating this policy using ICT Form (acknowledgement of receipt of ICT policy), which shall be returned to the ICT officer duly signed and acknowledged. The employee statement shall be deemed to be a legal document of Mitooma district local government.

3.6. SANCTION

Violation of the provisions of these policies and guidelines will result in severe disciplinary action as per the Uganda public service standing orders and may include termination of employment.

4. THE ICT STEERING COMMITTEE

The ICT steering committee consisting of seven (7) officers shall be assigned tasks of carrying out review, enforcement, monitoring and evaluation of the policy. A monitoring framework shall be developed by the said committee to ensure midterm review of the policy.

4.1. ROLES OF THE ICT STEERING COMMITTEE

a) Develop appropriate strategies for M & E of this policy. I.e. provide a strategic direction and priorities for Information and communication Technology management.
b) Review, approve, and make recommendations concerning ICT management, policies, procedures and standards.
c) Provide ongoing oversight over large ICT projects and initiatives
d) Recommend course of action in instances of noncompliance to set standards and policies.
f) Carry out annual evaluation on the implementation of the policy; and define short, medium and long term interventions based on the outcomes of the M & E reports

4.2. COMPOSITION OF THE ICT STEERING COMMITTEE

Deputy Chief Administrative Officer	Chairman
Information Technology Officer	Secretary
Chief Finance Officer	Member
Procurement Officer	Member
Internal Auditor	Member
Planner	Member
Communications Officer	Member

5. APPENDICES

5.1. ICT EQUIPMENT INVENTORY FORM

No.	Item descriptions	Model	Serial No.	Asset code	Date of purchase	Supplier	Location	User

Approved by;..... Date:.....

ICT officer

5.2. APPROVAL OF INSTALLATION AND USE OF NEW SOFTWARES

a) New software details

No.	Software descriptions	License code or serial No.	Date of purchase	Supplier(author)	User (Name and sign)

b) Software installation and use

Reasons for installation of new software:.....

.....

.....

.....

.....

Tested and approved by:..... Date:.....

ICT Officer

5.3. APPROVAL TO ACCESS ICT SYSTEMS

Details of a person

No.	Name	Title	Email address

Access approval (specify): IT room/Network resources/Email/Internet/others

Reasons for granting access;.....

.....

.....

.....

Approved by;..... Date;.....

ICT officer

5.4. ACKNOWLEDGEMENT OF RECEIPT OF ICT POLICY

I …….... (Name), agree that I will abide by the guidelines set forth in the above ICT policy. I also agree to the following: -

1. I have received a copy the ICT policy for the Mitooma district local government and I have fully read and understood it. I will adhere to the guidelines set forth in the subject.

2. I have noted that any violation(s) of these policies will be documented and brought to the attention of the District Chief Administration Officer for disciplinary action and may lead to termination of employment.

Employee signature:.....

Employee Name:..... Department.....

Date;.....

6. REFERENCES

i. The National ICT policy at https://ict.go.ug>ict-poliy-2014
ii. The National Information Technology Authority Act at https://www.nita.go.ug>publication
iii. The Computer Misuse Act (2011) accessible at http://www.ict.go.ug/resource/computer-misuse-act
iv. The Electronic Transactions Act (2011) accessible at http://www.ict.go.ug/resource/electronic-transactions-act
v. The Access to Information Act (2005) accessible at http://www.ulrc.go.ug/content/access-information-information-act-2005