BUSHENYI DISTRICT LOCAL GOVERNMENT ICT POLICY

ICT POLICY AND PROCEDURES

1. **Acceptable and Un acceptable Use of ICT Resources**
2. **Internet usage**
3. **ICT Security**
4. **Management Information Systems**
5. **Procurement and Disposal of ICT equipment**
6. **Maintenance and Repair**

ACRONYMS

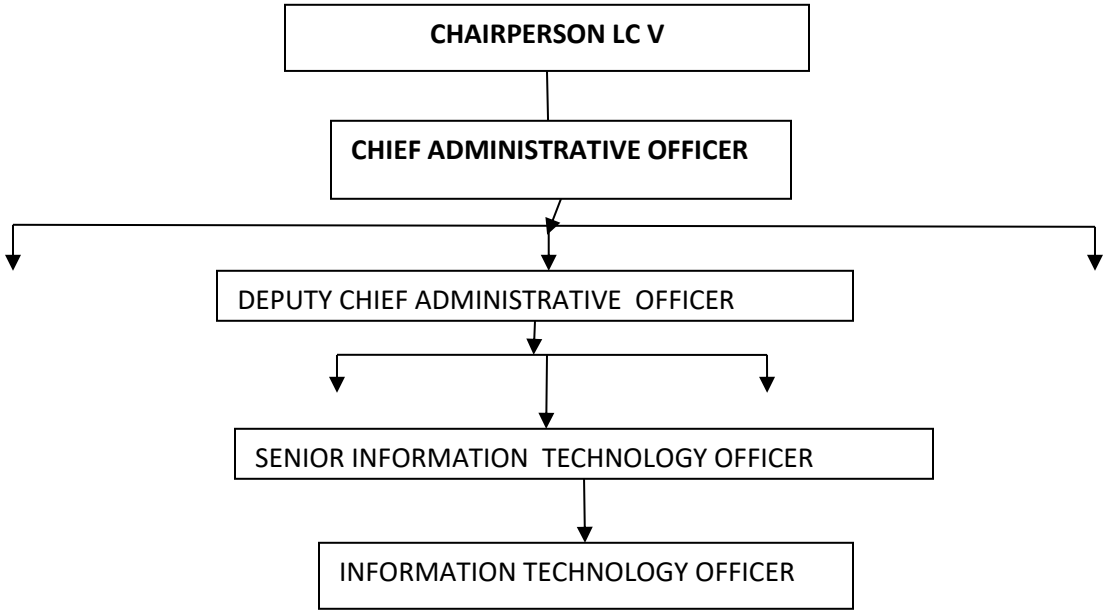
ICT	Information Communication Technology
PC	Personal Computer
IT	Information Technology
LLG	Lower Local Government
MIS	Management Information Systems
IPPS	Integrated Public Payroll System
IFMS	Integrated Financial Management Systems
PBS	Program Budgeting System
CAO	Chief Administrative Officer
SLA	Service Level Agreement
BDLG	Bushenyi District Local Government
LAN	Local Area Network
WAN	Wide Area Network
VPN	Virtual Private Network
ISP	Internet Service Provider
NITAU	National Information Technology Authority Uganda
LG	Local Government

TABLE OF CONTENTS

BUSHENYI DISTRICT LOCAL GOVERNMENT

ORGANISATIONAL STRUCTURE

Extracted Structure showing where IT officers lie on BDLG staff structure



FOREWORD

The policy is a recognition that Information, Communication and Technology are a hub of sustainable human development. Bushenyi district local government realizes that it needs to enhance communication and be able to communicate with the outside world through sharing of information by the use of Electronic Devices such Computers, Laptops, Smart Phones and I-Phones through Network

The policy therefore, seeks to define how the ICT at Bushenyi District Local Government will be used and managed. The use will be by staff, client and stakeholders.

It is the responsibility of the staff, stakeholders and clients to see to it that the Information, Communication and Technology in place is utilized with the maximum care and used responsibly.

JAFFARI BASAJJABALABA
DISTRICT CHAIRPERSON
BUSHENYI DISTRICT LOCAL GOVERNMENT

ACKNOWLEDGEMENT

Today Information Technology is one of the drivers of development. Without information and communication, you are kept outside the globe. Starting from a phone, you are communicating and making business from home.

Bushenyi District Local Government is desirous to use the Information Communication Technology to spur development of the district through quick service delivery to the community.

So the delivery of service through Information Communication Technology has to be used in a principled manner in order to spur this development. However, technological advancements like the Internet have digitally broken the geographical, physical, political and even sociological divide, transforming the world into a „Global Village. As a result, cyber-crime is progressively increasing. This calls for regulated and guided interventions to address the ICT related issues.

To this end, I thank the district technical staff and the District Council for providing funds to come up with this policy. I hope once this policy is implemented with the utmost guidance it requires, the District will deliver services to her people in the most effective and efficient manner.

MAHABBA MALIK
CHIEF ADMINISTRATIVE OFFICER
BUSHENYI DISTRICT LOCAL GOVERNMENT

EXECUTIVE SUMMARY

The utilization of Information and communication Technology (ICT) is on the rise in both public and private sector to embrace E-Governance. Bushenyi District Local Government has embraced E-governance in order to meet its mission, goals and objectives in a more effective manner by speeding up service delivery processes. The purpose of this policy is to establish acceptable and unacceptable use of ICT Equipment and network resources with its established culture of ethical and lawful behavior, openness, trust and integrity in order to maintain the confidentiality, integrity and availability of its information assets. This policy requires users of information assets to comply with organization policies. Bushenyi District ICT policies include Acceptable and un acceptable use of ICT resources policy, Internet usage policy, ICT security policy, Management Information Systems Policy, Procurement and Disposal of ICT equipment policy, Maintenance and repair policy.

1.0 INTRODUCTION

1.1 Policy Overview

1.1.0 Rationale for the ICT policy

Recent technological advancements like the Internet have digitally broken the geographical, physical, political and even sociological divide, transforming the world into a "Global Village". As a result, cyber-crime is progressively increasing. This calls for regulated and guided interventions to address the ICT related issues.

The utilization of IT (Hardware, Software and E-Applications) is on the rise in both public and the private sector. There is need for proper laws and guidelines to be developed to guide its utilization.

The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network recourses at Bushenyi District Local Government in conjunction with its established culture of ethical and lawful behavior, openness, trust and integrity.

Bushenyi District Local Government provides computer Devices, Networks, and other electronic information systems to meet missions, goals, and initiates and must manage them responsibly to maintain the confidentiality, integrity and availability of its information assets. This policy requires the users of information assets to comply with organization policies and protects the organization against damaging legal issues.

1.2 Policy Philosophy

Through Information Technology the District aims to prepare staff to participate in a rapidly changing world. Increased ICT skills promote independent learning and give greater access to a wide range of ideas and experiences. It enhances the quality of staff's work across their operations and should enhance and enrich the service delivery process in the district. All staff from support staff to Officers have access to information and communications technology

1.3 Vision

Having a prosperous population readily accessing quality ICT Services

1.4 Mission

Provision of quality ICT services for effective social transformation of our communities

1.5 Policy Goal

To guide the optimal development and utilization of ICT in the district

1.6 Policy Objectives

The staffs are encouraged to develop confidence in using hardware and software and other IT equipment.

- To use ICT to manipulate and present written work, images and sounds to convey information effectively.
- To promote widespread use of IT applications in both public and private sectors to enhance efficiency and effectiveness in service delivery.
- To store information, retrieve it and present it in ways which enhances interpretation and analysis
- To be aware of the role of ICT in the control of equipment encountered in daily life
- To be able to discuss the use of ICT and its place within real contexts
- Through providing appropriate experiences, staff will achieve ICT competence, acquiring knowledge about the application and implications of ICT, the necessary skills to apply ICT in a variety of contexts and a better understanding of the role and potential of ICT
- To sensitize communities about IT services as well as promotion and awareness campaigns in the communities.

1.7 Policy scope

All employees, intern students, contractors, consultants, temporary and other workers at Bushenyi District Local Government, must adhere to the policy.
The policy applies to information assets owned or leased by Bushenyi District Local Government, or to devices that connects to the District Council network or reside at Bushenyi District Local Government website.
ICT Committee must approve exceptions to this policy in advance through getting approval from ICT Officer.

2.0 POLICY

2.1 Acceptable and Un acceptable Use of ICT Resources

Bushenyi District has invested in information and Communication Technology infrastructure in an effort to improve its operations and administrative functions while enhancing E-Governance. The District considers ICT resources to be a valuable asset whose use must be managed to ensure integrity, availability, and security for lawful administrative and operational purposes.

While the district seeks to promote wide usage of ICT resources, guidelines must be in place so that users use them responsibly.

2.1.1 Scope

This acceptable use of ICT resources applies to all users of the district headquarter offices and LLG's. The resources referred to in this policy include but are not limited to the following.

1. District and LLG's Computers and related peripherals (printers)
2. The databases
3. Management information systems
4. The network and related network services
5. Any other system that may be installed to provide a service to the District or sub county.

2.1.0 User responsibilities

Bushenyi District ICT resources are providing primarily to facilitate a persons' 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 basic maintenance plus availing the resources to other users when needed.

Acceptable use of the District ICT resources may include

i. Use for data entry, analysis, storage and retrieval.
ii. Use for data management
iii. Use for communication purposes.
iv. Use for official business, like preparation of reports, minutes, presentations etc;

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

1. Attempt to access computers and other resources for which an individual is not authorized.
2. Unauthorized access to another user's files.
3. Attempt to break into or damage computer systems within the network or in other connected networks or individually at the district or sub county.
4. Attempt to circumvent Network Access Control, including by passing proxies and firewalls
5. Monitoring or interception of network traffic without permission
6. Probing for security weakness of systems by methods such as port scanning, password cracking without permission.
7. Un authorized extension or retransmission of network or network traffic including the installation of unauthorized wireless access points, routers or switches.
8. Unauthorized modification of District or/ and sub county data.
    - Unauthorized download, installation or running of programs or utilities that may flood the network causing denial of services to other users.
    - Sharing of network access credential with third parties for purposes of defeating network authentication.
    - Using the network to break into other networks
    - Creation, retention, downloading or transmission of any offensive, obscene or indecent images or data capable of being resolved into obscene or indecent image or material.
    - Creation, retention, or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety.
    - Sending electronic mail that purports to come from an individual other than the person actually sending the message using for example a forged address.
    - Using the resources for unsolicited advertising or transmission of electronic mail with intent to defraud often referred to as "spamming"
    - Deliberate activities that may result into one of the following;
        - ✓ Denying services to other users
        - ✓ Violating privacy of other users
        - ✓ Corrupting or destroying other users' data
        - ✓ Wasting of time on non-official activities

- Actions or inactions which intentionally or unintentionally aid the distribution of computer viruses or other malicious software.
- Download, install and use of un licensed software on the district computers and networks.

2.2 Internet usage

2.2.0 Social media

ICT provides a frame work for using social media like Facebook, WhatsApp, Twitter, YouTube, Website. It is a place where people exchange information, opinions and experiences to learn, develop and have fun. Whether users are handling district social media accounts or their own, they should remain productive.

The two elements of social media mainly include;

Using personal social media account

Users are allowed to access their personal accounts at the district and but are obliged to act responsibly and ensure that their productivity is not affected. Statements, views, comments on their accounts should not be used to represent views of entire district.

Using District social media account

Users are obliged to be respectful and polite when engaged in communication on the district social media account. Avoid deleting or ignoring comments. Never post defamatory, discriminatory, offensive or libellous content and commentary.

Avoid disclosing district confidential information through personal or district accounts.

2.2.1 Web content publishing

Bushenyi District works tirelessly to provide the best social services to its people in order to promote social economic development. To maintain and build upon that reputation, there is need to mind about the image we project. Web publishing policy exists to facilitate usability and consistency and to promote a standardized District with web site that correlate directly with sectors, departments, LLGs and the Public.

The District considers web publishing to be a key strategic resource for communication, planning, research, marketing and administration. 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 page content where the purpose and effect of the published information is in support of the District's mission.

web content publishing requirements

Accessibility

Bushenyi District web site must strive to adhere to web content accessibility guidelines of the world wide web consortium.

Redundancy

Do not repeat static information maintained elsewhere by the district.

Content Validity

- Bushenyi District Local Government controlled site must be registered under the bushenyi.go.ug domain.
- Content must be up to date and follow all sections of this policy and its supplements, as well as national law and codes.
- The District Information Officer with the help of the ICT Officer shall have 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.

Copyright

a) All district web page content should follow copyright laws
b) Publishers must have permission from any copyright holder to use text, photos, graphics, sounds, movies to which Bushenyi District does not hold copyrights.

2.2.3 E-mail usage

Electronic-Mail communication means a communication by means of electronic data messages over a network/internet.

Electronic messages that bear signatures shall be printed and filed for record purposes. Such information shall be acted upon pending the original message.

Phone messages shall have to be put in writing before such information is acted upon.

In order to avoid loss or damage to the electronic messages, the following are prohibited: -

- Sending spam via e-mail, text messages, pages, instant messages, voicemail, or other forms of electronic communication
- Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the receipt about the sender.
- Posting the same or similar non-business related messages to large numbers of UseNet newsgroup (newsgroup)

- Inappropriate use of IT equipment, including but not limited to supporting illegal activities, and procuring or transmitting material that violate the district policies against harassment or safeguarding of confidential or proprietary information.

2.3 ICT Security

Purpose

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

The District has made strong efforts to invest in establishing ICT infrastructure both at headquarters and lower level governments. The value of ICT investment accrues when users demonstrate responsible use of the Infrastructure. Poor usages result into faster breakdown of the ICT equipment 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 set, a laptop, printer in an office) or group (say in a computer pool room or server room) of equipment and that individual shall take the responsibility of ensuring its security

It is a requirement that whoever (staff, client and stakeholder) using the Bushenyi District Local government information technology devices should be responsible for its security, standard and leave it in good working condition. Where the device has developed a problem while in your use, please report it to the responsible Officer IT.

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

2.3.1 ICT Equipment Security

Scope

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

User Rules

1. Only authorized staffs and political leaders are permitted to open and use computers or related systems. Other staff, intern students, visitors shall access with permission/authorization from responsible officer.
2. No ICT equipment and other accessories shall be carried outside of the offices unless the responsible officer (The Chief Administrative Officer) has given explicit permission. As such equipment movement forms shall be put in place to facilitate this measure.
3. The I.T Officer shall maintain an asset register where such movements are monitored and tracked.

In order to enhance security of information and equipment of the ICT All equipment throughout the district shall be security marked and all security numbers or marks recorded in the inventory book.

All-important data or information has to be backed up on different files for future references.

Insurance should be covered through the district normal insurance arrangements. The system is backed up regularly and virus protection systems are in place.

In addition, staff and other Authorized persons of Bushenyi District Local Government shall be responsible for the security of the equipment, system and network traffic at the district.

To enhance security of our IT systems, the district shall build capacity for technical officers to enable them acquire IT security skills

Build a culture of security in district, public sector and the civil society through creating awareness within its populace on how to avoid and handle security risks.

2.3.2 Systems accounts

The systems accounts users are responsible for the security of data, accounts, and systems under their control. Passwords should be kept secure, accounts or passwords information not shared with anyone, including other personnel, family, or friends. Providing access to another individual, either deliberately or through failure to access, is a violation of this policy. As a security measure, all data has to be backed up on flash disks, portable external hard drives etc.

In cases where a computer is accessed by more than one person, several accounts are created with different access rights as it may be deemed necessary.

2.3.3 Data security.

The purpose of having data security, is to identify disseminate the District's framework 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 LLG's.

All this applies to all staff, intern students, volunteers, contractors, vendors or other affiliates of Bushenyi district with access to confidential institutional information.

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;

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

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 data protection and access.

The following policy statements thus apply;

1. All District data shall be stored on centrally maintained server while all LLG's data shall be maintained by each LLG's individually on their local computers with backup files kept with the district.

   In event that such data is stored on user desktops, laptops and other mobile devices, it is responsibility of the user to ensure its security, confidentiality and integrity in respect to this policy such as regular backup, password protection.
2. All access to data stored on central administrative databases must be through standard interfaces provided for by the various information systems (if any)
3. Requests for access to all administrative data and the central systems in general must be authorized by the relevant data owners (CAO, Planner, Finance officer, Principal personnel Officer and all other sector heads respectively). The granting of access is then effected by the officer responsible for managing ICT resources.
4. In 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.

5. Technical staff responsibility

The responsibility for protecting all important data stored in central district systems i.e. (servers, databases, network storage etc.) is a mandate of the ICT Officer with the guidance of 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 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 LLG's data shall be backed up and a copy of data of each be 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 can be retrieved any time in need. 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 annual basis and where appropriate, a formal Service Level Agreement (SLA) must exist with the off-site storage provider.

6. 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 back up media at a location remote from the processing center.
    - Approved Disaster Recovery Plan written and implemented to cover situations in which hardware/ or software cannot run in its normal environment.
7. 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, source of legal requirements should be as specified. ICT Officer under the guidance of the CAO is responsible for ensuring that these requirements are adhered to.
8. If any Database management system 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, and at any time.
    - Audit trails/ journals which record important activity
    - Control checkpoints

2.3.4 Use of passwords as security

District staff members must keep system level and user level passwords on their office computers secure to ensure confidentiality and integrity of data.

2.3.5: Prevention of Virus Infection to computers

All district computers must be installed with an Antivirus updated on weekly basis by the ICT officer. The District should have a fully installed internet and subscribed on monthly basis for this purpose.

2.3.6: Information proprietary

The district shall ensure that through legal or technical means that proprietary information remains within the control of Bushenyi district local government at all times. Conducting district business that results in the storage of proprietary information on personal or non-district controlled environment, including devices maintained by third party with whom district does not have a contractual agreement, is prohibited. This specifically prohibits the use of an e-mail account that is not provided by Bushenyi district local government or customer and partners, for organization business. Where a personal email is used for district work or information, the information has to be printed and filed with the district central registry. This in future will call for a district server where core district database shall have to be established such that core data or information can be accessed on personal E-mails in the district instead of moving files from one office to another.

Establishment of a server will be secured in a different room where access to the server shall be restricted to authorized persons.

Confidential data or information has to be encrypted if an Email is used to send that data.

2.3.7 Computing assets

Users are responsible for ensuring the protection of assigned district assets that includes the use of cable locks and other devices.

The district portable devices such as flash discs, external hard discs overnight must be secured or placed in locked drawers or cabinet. Promptly report any theft of district council property to management and ICT Officer at the district.

All PC's, Laptops and workstations must be secured with password-protected screensaver with the automatic activation features set to 10 minutes or less. The user must lock the screen or log off the device is unattended.

Devices that connect to the district network must comply with the minimum Access policy

Do not interfere with corporate device management or security system software, including but not limited to, antivirus, Windows, flash Disks, and removable hard disks.

District ICT officer shall be carrying out stock taking on all ICT equipment in the district and checking the status for every in a given financial year.

2.4 Management Information Systems

Management Information Systems like IFMS, YLPS, IPPS, and PBS require utmost care regarding access authorisation, data security and proper maintenance. Responsible Officers of these systems accounts shall ensure confidentiality of usernames and passwords to guard against unauthorised intrusion of these systems. The ICT Officer shall ensure that such systems are well maintained from time to time in collaboration with relevant ministries in charge of these systems

2.5 Procurement and Disposal of ICT equipment

Information and communication Technology equipment have an average useful life span of four years beyond which the equipment starts wear and tear though can still be used. Due to swift changes in technological advancements, there is need to change with new technology hence making ICT equipment after four years to be obsolete and thus calls for disposal.

Bushenyi District is obliged by law to implement a sustainable a procurement and disposal policy.

The ICT Officer shall be mandated with the monitoring and management of procurement and disposal of all district ICT equipment in liaison with the Procurement and Disposal Unit.

The district will maintain partnership with relevant procurement and disposal organizations like the National Environmental Authority (NEMA), Electronic waste collectors, ICT importers and assemblers, distributors and retailers.

Procedure for Procurement

The User department seeking to procure any ICT equipment shall seek for Technical specifications of the equipment from the ICT Officer in order to ensure quality standards of ICT equipment. On delivery, the ICT Officer must ascertain that the equipment has the required specifications.

Procedure for Disposal

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 current ICT inventory manually or electronically from the database

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

ICT equipment may be disposed of in the following ways;

- Recoveries from offices- Equipment identified for disposal during the annual ICT inventory stock-taking exercise may be salvaged and re-assembled. The refurbished computers may be placed in a pool of computers for allocation to new staff or a staff in need.
- Hard ware destruction- Obsolete hardware that may neither be salvaged, nor be sold, nor be donated may be destroyed. An inventory of hardware that is due for destruction or has been destroyed must be maintained. All hardware destruction should be done in accordance with available hardware destruction statutes or legal requirements.
- Hardware sale- Obsolete hardware may be sold at a salvage value. The District Board of Survey shall assess the hardware and attach the appropriate value for the hardware sale. All hardware for sale must be presented to ICT Officer for technical inspection to ensure that it doesn't contain any licensed software or District information.
- Hardware donations- Obsolete hard for donation to community outside the district shall follow guidelines laid down by the national policies on deployment of used technology equipment and environmental conservation. All hardware for donation should be presented to ICT Officer who will delete all information on the hardware before they are donated.

2.6 Maintenance and Repair

2.6.1 Professional Service Provider

The ICT equipment shall be managed, maintained and supported by secured professional service provider who shall offer quality service. The ICT Officer shall verify and certify the work carried out by the service provider in this case. The ICT Officer also gives support on occasions but this should not be the norm.

2.6.2 Basic Maintenance and repair

Users of Bushenyi District LG are obliged to carry out basic care on ICT equipment in their custody like avoiding exposing the equipment to dust and moisture. They should avoid packing heavy loads on top of them. There is need to cover them when not use and ensuring proper aeration

2.6.3 Scheduled and unscheduled maintenance and repairs

Scheduled maintenance will be triggered by the approach of a standard's review date. In such cases, the ICT Officer will develop a proposal to initiate a review of the standard two months before the review date occurs.

Unscheduled maintenance is usually precipitated by an unexpected or unique event such as: accidental breakdown, unforeseen failure of the equipment etc.

Maintenances and compliance purposes, authorized personnel shall monitor and Audit equipment, systems and network traffic. Devices that interfere with other devices or user on the district network may be disconnected. Information security prohibits actively blocking authorized audit scans. Firewalls and other blocking technologies must permit to the sources.

3.0 ICT COMMITTE

The I.T Committee consisting of seven (7) Officers shall be assigned tasks of carrying out review, enforcement, monitoring and evaluation of the policy. A monitoring frame work shall be developed by the said committee to ensure midterm review of the policy. The policy shall receive a midterm review every after five (5) years and full review every after ten (10) years. The analysis of annual ICT needs and usage survey realized during annual IT equipment stock taking shall be used as a basis for review on availability of new needs or information.

The appointed members of the Committee shall be.

1. Principal Assistant Secretary – Chairperson
2. Chief Finance Officer – Member
3. Senior procurement Officer – Member
4. Information Officer – Member
5. Senior Planner - Member
6. Senior Assistant Secretary – Member representing Sub-counties
7. Principal Assistant town clerk – Member Representing Town Councils
8. Information Technology Officer – Secretary

4.0 ADOPTION AND ENFORCEMENT

The policy shall be adopted as soon as it is discussed with District Technical Planning committee (TPC), Finance and Administration standing Committee and District Executive Committee (D.E.C) and then approved by district Council. The ICT Committee is responsible for enforcing this policy.

The ICT committee is responsible for dissemination of this policy and orientation of staff in ICT policy

The Committee shall put in place disciplinary measures on those staff (users) who do not conform to this policy like withdrawal of the equipment usage from a user who doesn't adhere to set guidelines if decided by the said committee.

5.0 GLOSSARY

User	A staff who is allocated or to whom a particular ICT resource was issued to.
Visitor	A staff who wants to have access and use an ICT resource that is not allocated to him/her.
Off-site buildings.	Out of the official District headquarter building or sub county office
Obsolete	An ICT resource is obsolete if its functionality is too minimal to meet demands by that particular user's requirements.
ICT Policy	A set of guidelines designed to regulate ICT equipment access, usage, maintenance, disposal and internet.
MIS	Management Information system is a set of interlinked databases designed to allow a user enter large amounts of data, store it, analyze it and that data can be retrieved on user's request.
E-governance	Administration that is based on electronic devices/Computing devises to speed up processing of systems.
E-mail	A communication by means of electronic data messages sent over a network/Internet.

6.0 REFERENCES

1. Computer misuse act, 2011
2. National Information Technology Policy, February, 2010
3. Robin Petch, (April 2004), paisley primary school - ICT policy
4. The electronic transactions act, 2011