MBARARA DISTRICT LOCAL GOVERNMENT

ICT Policies and Procedures 2011

Policy Outline

1. Acceptable Use of Information and Communication Technology Resources
2. Data Security
3. Physical Information & Communication Technology Security
4. Disposal of Information and Communication Technology Equipment (Electronic – waste management)
5. Web Content Publishing

CONTENTS

CONTENTS 2
ABBREVIATIONS 3
FOREWORD 4
ACKNOWLEDGEMENT 5
POLICY 1: Acceptable Use of Information and Communications Technology Resources 6
USER RESPONSIBILITIES: 6
POLICY 2: Data Security 9
USER RESPONSIBILITY 9
TECHNICAL STAFF RESPONSIBILITY 10
POLICY 3: Physical Information & Communications Technology Security 12
POLICY 4: Disposal of Information and Communication Technology Equipment (Electronic – Waste management) 13
Glossary of terms 15
POLICY 5: Web Content Publishing 16
WEB CONTENT PUBLISHING REQUIREMENTS 16

ABBREVIATIONS

CAO - ----- Chief Administrative Officer

E- WM ---- Electronic Waste Management

ICT - ------- Information Communications 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

FOREWORD

Mbarara district local government has embraced developments in ICT. In a bid to meet the National ICT policy 2003 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 information 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 equipments 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 telephony 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 level. 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.

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.

……

Baryomunsi Godfrey

VICE CHAIRPERSON MBARARA DISTRICT LOCAL GOVERNMENT

ACKNOWLEDGEMENT

This District Information and Communications Technology (ICT) Policy was developed with consultations from all sector and departmental heads reviewed through Technical Planning Committee and the planning unit with guidance from the Senior information scientist.

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 action to realize the intended objectives to promote social – economic development in the district.

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

……..

Lubuuka David

CHIEF ADMINISTRATIVE OFFICER/ MBARARA DISTRICT

POLICY 1: Acceptable Use of Information and Communications Technology Resources

PURPOSE:

Mbarara 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.

SCOPE

This acceptable use policy applies to all users of the District headquarter offices and Sub County 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 and Sub County 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 District or Sub County.

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 and Sub County Staff, Political Leaders, Intern students and some individuals granted permission to use resources. The definition also covers any individual who connects, attempts to connect to the District network whether from within the District or from remote locations.

USER RESPONSIBILITIES:

Mbarara District ICT resources are provided 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 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 or sub county.

ii. Attempt to access computers for which the individual is not authorized.

iii. Unauthorized access to another user's files.

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 data.

- Unauthorized download, installation or running of programmes 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 or any 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.
- Intellectual property rights infringement, including copy right, trademarks, patent, design and moral rights.
- 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 unauthorized access to networked resources, local or remote.
- 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.
- Actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software:
- Download, installation and use of unlicensed software on the district network and computers

POLICY 2: Data Security

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.

SCOPE

This policy applies to all staff, intern students, Vendors, Volunteers, Contractors or Other affiliates of Mbarara 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:

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 protection and access. The following policy statements thus apply:

1. 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.

2. All access to data stored in 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 Owner (i.e.CAO, Planner, Finance Officer, Principal Personnel Officer and all other Sector Heads respectively. The granting of access is then affected by the Officer responsible for managing ICT resources.

4. 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.

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.

5. 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.

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 backup media at a location remote from the processing centre.

- Approved Disaster Recovery plan written and implemented to cover situations in which hardware and / 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, and source of legal requirement should be specified. The ICT Officer will be responsible for ensuring that these requirements are adhered to.
8. 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

POLICY 3: Physical Information & Communications Technology Security

PURPOSE

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

Preamble

The District has made strong efforts to invest in establishing ICT infrastructure both at headquarters and lower local governments. The Value of ICT investment accrues when users demonstrate responsible use of the infrastructure it starts to gradually breakdown 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 equipments shall be the responsibility of the ICT responsible Officer.

Scope

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

Policy Statements

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 computer equipment and other accessories shall be carried out of the Offices unless the responsible Officer has given explicit permission. As such Equipment movement forms shall be put in place to facilitate this measure.

3. The ICT Officer shall maintain an asset register where such moves are monitored and tracked.

POLICY 4: Disposal of Information and Communication Technology Equipment (Electronic – Waste management)

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 by law 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 for equipment like computers may be salvaged to assemble a functional equipment like personal computer, which may then be re- deployed for use, donated or sold.

POLICY STATEMENT:

The ICT Officer shall be mandated with the monitoring of acquisition and management of disposal of all council 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, refurbishers, ICT Importers and assemblers, distributors and retailers.

All District user departments and LLGs shall be required to avail obsolete ICT equipment to the responsible Officer for disposal.

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 off 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 advice on the appropriate market price for the hardware sale. The Finance department may also 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 policies 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 council 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.

Glossary of terms

Consumers 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, and may feed into the second – hand market directly or through refurbishers.

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.

E – Waste 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.

POLICY 5: Web Content Publishing

PURPOSE

Mbarara District has worked hard to provide social services to its people to promote Social 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 Web site that correlate 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 a periodic basis.

SCOPE

Any Web document that represents Mbarara 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.

POLICY STATEMENTS:

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.

WEB CONTENT PUBLISHING REQUIREMENTS

Accessibility

Mbarara District web site must strive to adhere to the Web Content Accessibility Guidelines of the World Wide Web Consortium. These guidelines are required of all Web sites, regardless of any written exception approvals of other restrictions in the Web standards and Guidelines.

Redundancy

Do not repeat static information maintained elsewhere by the District.

Content Validity

i. Mbarara District Local Government controlled site must be registered under the Mbarara.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.

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 Mbarara District does not hold copyrights