REPUBLIC OF RWANDA

EASTERN PROVINCE

KAYONZA DISTRICT

P.O. Box: 3 RWAMAGANA

WEB SITE: www.kayonza.gov.rw

E-mail : kayonzadistrict@kayonza.gov.rw

ICT ACCEPTABLE USE POLICY

Organized
By
Eng.Gatete N. Augustine
Systems & Network Administration-Kayonza District.

1

TABLE OF CONTENTS

CONTROL DOCUMENT

THIS DOCUMENT WAS PREPARED BY SYSTEMS AND NETWORK ADMINISTRATOR TO FACILITATE

IT PRACTICE IN THE DISTRICT

ENG.GATETE N. AUGUSTIN

Network & System Administrator

AUTHORIZATION

RURANGWA Jean Paul	**KAGABA Hero Aaron**
Dir. Hr & Administration of Kayonza District	District Executive Secretary

DISTRIBUTION

Kayonza District

1. ICT POLICY

1.1 Introduction

Information and Communication Technology (ICT) and the Internet are widely available to staff in KAYONZA DISTRICT OFFICES. The District's technology services offer vast, diverse and unique resources to users providing access to:

- *Computers to process data, save data, speed up, and facilitate service delivery*
- *Information and Communication Networks: providing shared network resources and applications.*
- *Internet Access: providing global information and social networking*
- *E-Mail: providing opportunities for electronic interpersonal communication*
- *Emerging applications to be adopted as appropriate.*

The District policies, regulations establish rules for behavior and communication applicable to the use of ICT networks and the Internet. Individuals are responsible for their actions while using the ICT and the Internet. The use of such technology is a privilege not a right. Inappropriate use may result in restrictions or cancellation of access rights and/or further disciplinary action.

1.2 POLICY STATEMENT

"It shall be the responsibility of the I.T. Department to provide adequate protection and confidentiality of all corporate data and IT tools and accessories such as Computer desktops and laptops, held at Kayonza District, to ensure that these devices are well maintained. Information and Communication Technology (ICT) is provided to support District activities. Computers and other ICT facilities may face security breaches that can compromise confidential information and expose the District to losses and other legal risks".

1.3 ART 1: REASON OF ICT POLICY?

Accordingly, to the internal organization of District, is created an acceptable use of technology resource policy (AUP) of Kayonza District

1.4 ART 2: AREA OF EXECUTION

The set is established in Kayonza District, Eastern Province only.

1.5 ART 3: DURATION

These internal rules are constituted for unspecified duration.

1.6 ART4: AMEND

This policy is maintained by the ICTk Office. Requests to change the policy should be made to the Mayor. All changes will need to be approved by District Management team and ICT/MIS Officer.

1.7 ART 5: MONITORING AND PRIVACY ISSUES

Communications via ICT resources are often public in nature and general District rules for behavior and communications apply. It is expected that users will at all times comply with district standards and will act in a responsible and legal manner, in accordance with district standards, as well as with government laws.

It is important that all users and staffs understand that the district, *as the owner of the ICT resources, reserves the right to monitor and review* the use of these ICT resources. The district intends to monitor and review in a limited fashion, and will do so as needed to ensure that the systems are being used for district-related administrative and service delivery purposes. The Mayor or executive comity or District council reserves the right to eliminate personal use of the district's ICT resources by any or all employees at any time.

1.8 ART 6.OBJECTIVE

Information technology resources are valuable assets provided to enhance the core functions of administrative staffs. The use of the District's information technology resources is a privilege extended to

authorized users for service, and administration. This **ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES POLICY (AUP)** governs the use of the District's information technology resources in an atmosphere that encourages free exchange of ideas and an unwavering commitment to administrative freedom. The District community is based on principles of honesty, integrity, respect for others, and respect for others' privacy and property.

1.9 ART 7: WHAT THE DISTRICT SEEKS TO?

- *Protect the confidentiality and integrity of electronic information and privacy of its users, to the extent required or allowed under government law.*
- *Ensure that the use of electronic communications complies with the provisions of District policy and government law.*
- *Allow for the free exchange and working environment of ideas and support of administrative freedom.*

The District cannot protect users from the presence of material they may find offensive. The presence of such material must not be represented as an approval by the District.

This policy applies to all staff, administration agents and others, referred to as users throughout this policy, while accessing, using, or handling the District of Kayonza's information technology resources. In this policy, "users" include but are not limited to subcontractors, visitors, and

contract support personnel, media representatives, guest speakers, and non-district entities granted access. All "users" are required to be familiar with and comply with this policy.

1.10 ART 8. SCOPE/RANGE

1.10.1 INDIVIDUALS COVERED

In this policy, “users” are those who access, use, or handle the District’s IT resources. They include, but are not limited to: training in service, staff, subcontractors, visitors, visiting staff, and contract support personnel, media representatives, guest speakers, and non-District entities or individuals who are granted access.

1.10.2 RESOURCES COVERED

This policy applies to all District IT resources, whether individually controlled, shared, stand-alone, or networked. It applies to all Hardware and software such as computers, photocopiers, printers, communication Devices, and all other electronic facilities owned, leased, operated, or provided by the District or otherwise connected to District IT resources.

1.11 ART 9: CONFORMITY

At minimum, individual District units must follow these principles and rules while connected to District IT resources. Each unit is responsible for security on its systems.

1.12 ART10: GENERAL POLICY

All users are expected to comply with District IT security policies and follow IT security best practices where possible.

1.13 ART11: PRIVACY

1.13.1 USER PRIVACY

The District provides electronic resources to users to help the District fulfill its mission. The District routinely monitors electronic hardware, data, software, and communications. There should be no expectation of privacy for any information stored, processed, or transmitted on District IT resources.

1.13.2 DISTRICT RIGHTS

Users should be aware that any activity on systems and networks may be monitored, logged, and reviewed by District approved personnel (ICT Officer) or may be discovered in legal proceedings. All documents created, stored, transmitted, or received on District computers and networks may be subject to monitoring by systems administrators.

The District reserves the right to access, monitor, review, and release the contents and activity of an individual user's account(s), including staff mail or other administrative mail, on any account on any District-owned or non- District -owned resource on or off District property connected to District networks. This action may be taken to maintain the network's integrity and the rights of those with

authorized access, to safeguard against threatened security of a computer or network system, to protect from other suspected misuse of District resources. Prior approval from the Information Security Office (ISO) or another authorized government office (such as the Office of RDB, Audit and Consulting Services) or court order must precede this action.

1.14 ART 12: USER RESPONSIBILITIES

1.14.1 USERS MUST:

- **RESPECT AND PROTECT THE PRIVACY OF OTHERS.**

a. Use only assigned accounts.
b. Not view, use, or copy passwords, data, or networks to which they are not authorized.
c. Personal information such as names and addresses and telephone numbers should remain confidential when communicating on the system. Staff should never reveal personal information.
d. Users should notify the district IT or other staff whenever they meet information or messages that are dangerous, inappropriate to the system.
e. Not distribute private information about others or themselves.

f. Users shall not seek information on, obtain copies of, or modify files, other data or passwords belonging to other users, or lie other users on the system, or attempt to gain unauthorized access to the system.

- **Respect and protect the integrity, availability, and security of all electronic resources.**

a. Observe all stands alone computer, printer, photocopier, network security practices, or other ICT device as posted.
b. Report security risks or violations to ICT officer or other administrator.
c. Not destroy or damage data, networks, or other resources that do not belong to them, without clear permission of the owner.
d. Conserve, protect, and share these resources with other employees and ICT users.
e. Use all ICT facilities only for District interest.

1.14.2 USERS WILL:

a. Comply with District policies and follow District best practices where possible to maintain the confidentiality, integrity, and availability of computer systems and information on all devices under their control.

b. Make regular backups of information and files as appropriate.

c. Control and secure physical and network access to IT resources, data and Report threatening or discomforting materials to ICT officer.

d. Properly log out of sessions.

e. Monitor access to their accounts. If a user suspects unauthorized activity or that their account has been compromised, they must report it and change passwords immediately.

f. Install, use, and regularly update virus protection software.

g. Where technically possible, abide by the password protection best practices specified for each IT resource.

h. Use only the passwords and privileges associated with their computer account(s) and use those account(s) only for their authorized purpose.

i. Respect and honor the rights of other individuals with regard to intellectual property, privacy, freedom from harassment, academic freedom, copyright, and use of IT resources.

j. Use District provided software in a manner that strictly adheres to all licensing provisions, including installation, use, copying, number of simultaneous users, and other terms of the license.

1.14.2 USERS WILL NOT:

a. Provide access codes to any unauthorized user.

b. Use accounts, access codes, privileges or IT resources for which they are not authorized.

c. Tamper, modify, or alter any restrictions or protections placed on their accounts, the District system, or network facilities.

d. Physically damage or vandalize IT resources, or use IT resources to damage other District resources or systems.

e. Use of the system to access, store, or distribute obscene, pornographic or inappropriate material is prohibited.

f. bring Food and beverages in office as well as on computer table or where other ICT facility stands alone.

g. Commit copyright infringement, including file sharing of video, audio, or data without permission from the copyright owner.

h. Use IT resources to introduce, create, or propagate computer viruses, worms, Trojan horses, or other malicious code.

i. Obtain extra IT resources or gain access to accounts for which they are not authorized.

j. Eavesdrop on or intercept other users' transmissions.

k. Attempt to degrade the performance or availability of any system or to deprive authorized users access to any District IT resources.

l. Misrepresent their identity with actions such as IP address "spoofing," email address falsification, or social engineering.

m. Send email chain letters or mass mailings for purposes other than official District business.

n. Use District resources to relay mail between non-District email systems.

o. Comment or act on behalf of the District over the Internet without authorization.

p. The system IT is a district facility and may not be used to support or oppose political candidates or ballot measures.

q. Use of the system for commercial solicitation is prohibited. Use of the system for charitable purposes must be approved in advance by the Superintendent or designee.

r. Connect devices (such as switches, routers, hubs, computer systems, and wireless access points) that are not approved by the ICT of District or institutional IT organization to the network.

s. Use without authorization of District ICT office any device or application that consumes a disproportionate amount of network bandwidth.

t. Respond to electronic requests (email, instant message, text message, etc.) that ask for generally protected information, such as passwords, social security numbers, or credit card numbers.

u. Install or download software on internet.

v. Deliberately visit, view, download, print, copy, forward or otherwise transmit any unlawful material. If you mistakenly access such material you should notify ICT department. You should be aware that you will be held responsible for any claims brought against the District.

1.15ART 13: COPYRIGHT

1. The unauthorized installation, use, storage, or distribution of copyrighted software or Materials on District computers is prohibited.

END