**REPUBLIC OF KENYA**


**COUNTY GOVERNMENT OF MACHAKOS**

**DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY**

# COUNTY ICT POLICY

# SEPTEMBER 2021

**TABLE OF CONTENTS**

**TABLE OF CONTENTS** ..... i

**GLOSSARY OF TERMS** ..... iii

**1.0 INTRODUCTION** ..... 1

**1.1 Background** ..... 1

**1.2 Vision and Mission Statements** ..... 2

**1.3 Status of ICT in Machakos** ..... 3

**1.4 ICT SWOT Analysis** ..... 4

**1.5 The Legal Framework** ..... 5

**2. CHALLENGES OF ICT IN COUNTY DEVELOPMENT** ..... 6

**2.1 Introduction** ..... 6

**2.2 Lack of Adequate Policy, Legal and Regulatory Framework** ..... 6

**2.3 ICT Infrastructure** ..... 6

**2.4 Human Resource Development** ..... 7

**2.5 Limited Universal Access** ..... 7

**2.6 Limited Public-Private Partnerships (PPP)** ..... 8

**2.7 Limited Service Automation** ..... 8

**2.8 Non-Prioritization of ICT** ..... 8

**3. INFORMATION TECHNOLOGY** ..... 9

**3.1 Introduction** ..... 9

**3.2 Policy Objectives** ..... 9

**3.3 Strategies** ..... 10

**3.3.1 Information Technology Infrastructure** ..... 10

**3.3.3 Services Automation** ..... 11

**3.3.4 E- Learning** ..... 11

**3.3.5 ICT in Health Services** ..... 12

**3.3.6 Fiscal Measures** ..... 12

**3.3.7 Environmental Issues** ..... 12
**4. POLICY GUIDELINES** ..... 13
**4.1 Email and Instant Messaging** ..... 13
**4.1.1 Objective** ..... 13
**4.2 Internet usage** ..... 15
**4.3 Password security** ..... 16
**4.4 Intranet usage** ..... 18
**4.6 Software usage and licensing** ..... 20
**4.8 Inventory and equipment** ..... 24
**4.9 Information security** ..... 26
**4.10 Remote access** ..... 30
**4.11 Privacy** ..... 31
**4.12 Service level agreements** ..... 33
**5. ACTORS / STAKEHOLDERS ROLES AND OBLIGATIONS** ..... 35
**5.1 The County Government** ..... 35
**5.2 The County Assembly** ..... 35
**5.3 ICT Steering/Governance Committee** ..... 35
**5.4 The ICT Department** ..... 36
**5.5 ICT Government Agencies** ..... 36
**6. TARGETED AUDIENCE ROLES AND OBLIGATIONS** ..... 38
**6.1 System users/Employees** ..... 38
**6.2 The General Public** ..... 38
**7. MONITORING AND EVALUATION** ..... 39
**7.1 Definition** ..... 39
**7.2 M&E Implementation Plan** ..... 39

**GLOSSARY OF TERMS**

Third party-means any other person who is not an employee of the County Government.

Certification Service Provider means a person who has been granted a license to issue electronic signature certificates.

Computer means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, software and communication facilities which are connected or related as a system or network;

Data Communications – Digital transmission of information between computers

E-commerce means the use of electronic networks to exchange business information, services, product and payments.

E-Government service means public service provided electronically by a Ministry or Government Department, local authority, or body established by or under any law or controlled or funded by the Government.

ICT (Information and Communications Technologies) means the technologies including computers, telecommunication and audio-visual systems, that enable the collection, processing, transportation and delivery of information and communication services to users.

Infrastructure – refers to an integrated system of facilities used to provide one or more ICT services.

Interconnection – refers to physical and logical linking of two separate networks so that customers of one network can reach and communicate with customers of the other network.

Internet means an interconnected system of networks that connects computers via the Transmission Control Protocol Internet Control Protocol (TCP/IP) and includes future versions thereof.

License – An authorization granted by a regulatory authority for the provision of ICT services or for use of the radio frequency spectrum.

Regulation means the process of ensuring that public utilities operate inaccordance with legal rules. These rules may govern the offering of service by an operator and includes practices, classification and definitions.

HDD refers to hard disk drive

IFMIS refers to Integrated Finance Management Information System

LAIFOMS refers to Local Authority Integrated Financial Operations and Management Systems

IPPD refers to Integrated Personnel and Payroll Database

Universal access refers to allowing everyone in the country to have access to ICT facilities within a reasonable distance and at a reasonable cost

Universal Service is a policy of the Government in making ICT services, including advanced ICT services available throughout the country at affordable prices so that they are either available or easily accessible to anyone whenever they are needed, regardless of their geographic or physical location, and with due regard to people with special needs.

## 1.0 INTRODUCTION

### 1.1 Background

The Government of Kenya, its citizens, have identified roles played by ICT in the social and economic development of the nation and thus promulgated a national ICT policy based on Kenya Vision 2030

This policy's objective is to provide a framework on the management of sectors within the county and guide related interactions within and beyond Machakos County. It shows the strategies on ensuring the County's residents and interested investors communicate and apply ICT in a structured way.

The policy addresses key issues and challenges in ICT as well as propose a wide range of measures and actions in response to them. It also seeks to provide a clear road-map for an integrated approach to planning and sustainable management of
ICT now, and for years to come.

The successful implementation of the objectives herein will firmly set the County on the path towards effective communication and the harnessing of ICT for the holistic development of its people.

The policy is based on four guiding principles: infrastructure development, human resource development, stakeholder participation and appropriate policy and regulatory framework.

## 1.2 Vision and Mission Statements

### Vision

The vision of the ICT department is to:

"Provide high quality, agile, innovation and robust value-for-money trusted ICT solutions which enable the county to be very effective and productive while putting the customer at the heart of all we do"

The vision is aligned to the county vision that aims at having a world class County with a high quality of life to all citizens in a clean and secure environment.

### Mission

The mission of the county is:

"To transform livelihoods through speedy, efficient, inclusive and sustainable development."

### 1.3 Status of ICT in Machakos

Prior to the formation of Machakos county government all the ICT functions were under the ministry of local government in collaboration with ministry of information.

**Machakos County Government ICT status.**

| Aspect | Current status |
|---|---|
| Aspect Current Status Infrastructure and Connectivity | • The County has a functional National OpticalFiber Backbone Infrastructure (NOFBI)<br>• Partial LAN or WAN<br>• The GSM connectivity is not reliable<br>Most of the departments have a functional LAN. WAN is available at all offices in Machakos town and at the Mavoko Sub county offices |
| Interoperability of Systems | • IFMIS system is operational (the payment module) but departments have to bring their manually approved payment vouchers to the head office;<br>• IPPD is used for payroll payment but is not connected to IFMIS. The transfers of salary vouchers are manual.<br>• LAIFOMS is used to collect revenue and is not connected to IFMIS |
| Human Resource and Capacity Building | • The number of staff in ICT department at the County Executive is 28 (including the Chief Officer); The County Assembly has adequate staff.<br>• Few institutions are available in the county to train on ICT |
| Environment and Legal Framework | • There is no legislation guiding the use of ICT within the county<br>• There are no specific policies to guide ICT use (subject to further review and confirmation) |

### 1.4 ICT SWOT Analysis

| STRENGTHS | WEAKNESSES |
|---|---|
| • Strong political good will of ICT<br>• Existing of National policy<br>• E-Governance<br>• Allocation of ICT Sector budget<br>• Strong Institutional Organization (ICT Authority)<br>• Free internet for Government (NOFBI) | • Lack of sufficient ICT Infrastructure<br>• Lack of awareness about ICT and the benefits of E-Governance<br>• Existing high rate of ICT illiteracy<br>• Inadequate financial resources |
| **OPPORTUNITIES** | **THREATS** |
| • National Optic fiber backbone infrastructure (NOFBI)<br>• Last mile power connection<br>• County connectivity project<br>• Digital literacy (Laptop for schools)<br>• According to Vision 2030, the economic impact of ICTs will be driven by the Business Process Outsourcing (BPO) sector and thus the Government as well as private sector are investing heavily on ICT.<br>• Establishment of modern county headquarter with modern ICT facilities<br>• Increment in budgetary allocation<br>• Increased employment<br>• Creation of ICT awareness forums | • Rapid technology change<br>• Potential ICT crimes and difficulty to control it<br>• Loss of job due to ICT automation<br>• Competition of available resources with other county departments |

The department of ICT was established in the year 2013 after devolution. Since its establishments, the department has achieved the following;

- Setting up CCTV surveillance security system
- Setting up wide area network (MPLS), local area network and internet
- Setting up Government website & email communication

### 1.5 The Legal Framework

The Constitution of Kenya 2010 under Article 6 creates county governments and the Structures spelt out in chapter 11. The County Governments Act of 2012 gave effect to Chapter11 of the Constitution to provide for County Governments, their powers, functions and responsibilities to deliver Services. In the delivery of services to the people, Chapter IX on Public Communication and Access to Information outlines the various ways the county government can disseminate information to populations and guidelines for the same.

## 2.0 CHALLENGES OF ICT IN COUNTY DEVELOPMENT

### 2.1 Introduction

The broad challenge is to harness the potential of ICTs for economic growth and poverty reduction. Specific challenges include lack of a comprehensive policy and regulatory framework, inadequate infrastructure, and insufficient skilled human resources.

### 2.2 Lack of Adequate Policy, Legal and Regulatory Framework

Currently, ICT issues are considered under various legislation including The Science and Technology Act, Cap. 250 of 1977, The Kenya Broadcasting Corporation Act of 1988 and the Kenya Communications Act of 1998, which are inadequate in dealing with issues of convergence, electronic commerce and e-Government. There is need for a comprehensive policy, legal and regulatory framework to:

a) Support ICT development, investment and application;
b) Promote competition in the industry where appropriate;
c) Ensure ICT is easily accessed
d) Address issues of privacy, e-security, ICT legislation and cybercrimes, ethical and moral conduct, copyrights, intellectual property rights and piracy;
e) Support research and development in ICT; and
f) Develop an institutional framework for policy development and review.

### 2.3 ICT Infrastructure

The lack of adequate ICT infrastructure has disenabled provision of efficient and affordable ICT services in the county. The affected infrastructure includes among others:

- ICT support infrastructure; such as networks, CCTV, unified communications,
- Software development, implementation and acquisition;

### 2.4 Human Resource Development

The County Government recognizes the role played by the various institutions providing ICT education and training. However, there is need to strengthen and implement the training through:

a) Promoting ICT training to the public by developing ICT hubs/ resource centers, digitizing libraries;
b) Establishing networks for sharing training resources; and
c) Developing strategies to support research and innovation.

### 2.5 Limited Universal Access

Access to ICT services is limited; thus, there is need to enhance universal access through.

a) Provision of adequate resources to the ICT department;
b) Developing the requisite ICT infrastructure;
c) Creating incentives for service providers to deploy services in rural and under-served areas;
d) Creating awareness of benefits of ICT to the public

### 2.6 Limited Public-Private Partnerships (PPP)

There is need for an enabling environment for Public-Private Partnerships (PPP) in ICT development for higher investments.

### 2.7 Limited Service Automation

A major challenge facing the County is to provide services in an efficient -effective way. Service Automation provides a framework for improved service delivery and enhanced communication and information provision within the County. Developing adequate capacity within the County to implement and realize the benefits of service automation is much needed. According to Vision 2030, the economic impact of ICTs will be driven by the Business Process Outsourcing (BPO) sector.

### 2.8 Non-Prioritization of ICT

There is need for sustained high level ICT championship at County level to provide oversight, inspiration and political goodwill. Effective leadership should facilitate the mobilization of resources to develop an ICT environment that is conducive to investments in the County.

## 3. INFORMATION TECHNOLOGY

### 3.1 Introduction

The rapid advancements and explosive growth in the field of information technology (IT) and of the information services sector have radically changed the world's economic and social landscape, which have given rise to a new society based on information and knowledge. These changes have further resulted in new avenues of development, employment, productivity, efficiency and enhanced economic growth.

The growth of IT was generally due to creating jobs, raising productivity, increasing income and opening many opportunities for increased trade and human development. The continuous use of information technology provides opportunities for new ways to creating wealth, which contribute to poverty mitigation.

The management recognizes that there is a growing digital split between the countries that are highly capable and developed in the field of information technology as well as between rural and urban areas in Kenya. Therefore, it is the objective of the government to initiate steps to reduce this split by using information technology to quickly develop all sectors of the economy.

The County Government therefore identifies information as a resource, which must be generated, collected, organized, leveraged, secured and preserved for county prosperity.

### 3.2 Policy Objectives

**The objectives of the County ICT policy include:**

a) Ensuring that ICT plays a key role as an enabling tool, addressing gaps relating to gender, youth, people with special needs, rural and urban and disadvantaged groups, and as a literacy tool for the population and potential users;

b) It uses ICT to achieve the objectives of reducing poverty, improving healthcare, and general welfare of the population;

c) Using e-service as a tool to improve internal efficiency and quality of public service delivery and help in the fight against corruption;

d) Encouraging the use of ICT in educational institutions in the county so as to improve the quality of teaching and learning;

e) Using ICT to generate additional employment and promoting entrepreneurship for the new digital economy;

f) Encouraging and accelerating investments and growth in ICT hardware, software, Internet, training, ICT enabled services, telecommunications and electronic commerce;

g) Providing adequate infrastructure in the county for ICT sector to flourish;

h) Using ICT to improve security;

i) Using ICT to promote among, labor, health, social welfare, sports, culture, water and natural resources;

j) Facilitating the development of sectoral ICT policies and strategies e.g. education, e-water, e-health, e-agriculture.

k) Address issues relating to cybercrime and how ICT is positioned to handle that.

### 3.3 Strategies

The County Government will implement the following strategies to apprehend the above objectives.

#### 3.3.1 Information Technology Infrastructure

The board of ICT will come up with methods to encourage the provision of infrastructure for access to county, national and international information resources.

### 3.3.2 Services Automation

The general goal of Services Automation is to make the County Government more result oriented, efficient and public centered. This Service Automation strategy will focus on redefining the relationship between County Government and the public with the objective of empowering them through increased and better access to government services.

The objectives of Services Automation will be to:

a) Improve teamwork within the County Government to enhance efficiency and effectiveness of resource consumption;

b) Improve competitiveness by providing timely information and delivery of County Government services;

c) Reduce transaction costs for the Government, public and the private sector through the provision of products and services electronically;

d) Provide an environment for public participation in Government activities.

### 3.3.3 E- Learning

The ICT policy will promote the growth and implementation of e learning by employing the following strategies:

- Promoting and facilitating the development of e-learning resources;
- Promoting Public - Private Partnerships to organize resources in order to support e-learning initiatives;
- Promoting the development of integrated e-learning curriculum to support ICT in education; polytechnics, ECDs.
- Providing affordable infrastructure to facilitate dissemination of knowledge and skill through e-learning platforms;

- Creating awareness of the opportunities offered by ICT.

### 3.3.4 ICT in Health Services

The use of ICT in health delivery systems highlights important human rights by improving equity and quality of life. Thus, the County will promote use of ICT in health delivery by:

i Providing ICT facilities in all public health facilities;

ii Providing automated health services

iii Providing ICT training to medical staff;

### 3.3.5 Fiscal Measures

The County Government will introduce measures to encourage increased investment and growth in the ICT sector so as to create a favorable investment climate for the development of a competitive ICT enabled economy.

The objectives will be:

a) To offer County ICT products and services at subsidized prices competitively;

b) To develop monetary tools that respond to the fast changing needs of the information economy;

c) To offer incentives to attract ICT investment;

d) To make budgetary provision to spur the growth of ICT.

### 3.3.6 Environmental Issues

The County will promote the use of environmental-friendly ICT products to address environmental and cost issues in line with County Solid Waste Management Policy.

## 4. POLICY GUIDELINES

### 4.1 Email and Instant Messaging

#### 4.1.1 Objective:

The policy provides appropriate guidelines for productively utilizing the county's email system and instant messaging technology.

#### 4.1.2 Applies to:

All county employees and other stakeholders.

#### 4.1.3 Key guidelines:

i The county has established this policy with regard to the acceptable use of county provided electronic messaging systems, including but not limited to email and instant messaging.

ii Email and instant messaging are important and sensitive business tools. This policy applies to any and all electronic messages composed, sent or received by any employee or by any person, using county provided electronic messaging resources.

iii The county sets forth the following policies but reserves the right to modify them at any time in order to support the county:

#### 4.1.4 General

**The county provides electronic messaging resources to assist in conducting county business**.

i. All messages composed and/or sent using county provided electronic messaging resources must comply with county policies regarding acceptable communication.

ii. The County prohibits discrimination in line with Article 27 of the Constitution.

iii. Upon termination or separation from the county, the county will deny all access to electronic messaging resources, including the ability to download, forward, print or retrieve any message stored in the system, regardless of sender or recipient.

iv. Each employee will be assigned a unique email account where applicable.

v. Employees authorized to use instant messaging programs will be advised specifically on which instant message program(s) are permissible.

vi. Employees authorized to use instant messaging programs will be assigned a unique instant messaging identifier/username.

vii. Carefully consider how the recipient might interpret a message before composing or sending it.

viii. Any employee who discovers a violation of these policies should immediately notify the ICT Department.

ix. Any employee in violation of these policies is subject to disciplinary action.

### 4.1.5 Ownership

i. The email/electronic messaging systems are county property. All messages stored in county provided electronic messaging system(s) or composed, sent or received by any employee or non-employee are the property of the county.

ii. Electronic messages are NOT the property of any employee.

iii. The County reserves the right to intercept, monitor, review and/or disclose any and all messages composed, sent or received.

iv. The unique email addresses and/or instant messaging identifiers assigned to an employee are the property of the county. Employees may use these identifiers only while employed by the county.

### 4.1.6 Confidentiality

i. Messages sent electronically can be intercepted inside or outside the county and as such, there should never be an expectation of confidentiality. Do not disclose proprietary or confidential information through email or instant messages.

ii. Electronic messages can never be unconditionally and unequivocally deleted. The remote possibility of discovery always exists. Use caution and judgment in determining whether a message should be delivered electronically versus in person.

iii. Electronic messages are legally discoverable and permissible as evidence in a court of law. Messages should not be composed that you would not want to read out loud in a court of law.

iv. Employees are prohibited from unauthorized transmission of county trade secrets, confidential information, or privileged communications.

v. Unauthorized copying and distribution of materials is prohibited.

## 4.2 Internet usage

### 4.2.1 Objective:

This policy provides an appropriate guideline for accessing and utilizing the Internet through the county's network.

### 4.2.2 Applies to:

All employees with authorized access to Internet services

### 4.2.3 Key guidelines:

Internet services are authorized to designated employees by their manager to enhance their job responsibility. The Internet is an excellent tool but also creates security implications that the county must guard against. For that reason, employees are granted access only as a means of providing support in fulfilling their job responsibility.

### 4.2.4 General

i. Internet access is approved for designated employees by their immediate manager.

ii. Each individual is responsible for the account issued to him/her. iii. Sharing Internet accounts or User-ID's is prohibited.

iii. Organizational use of Internet services must reflect the mission of the county and support the county's goals and objectives.

iv. These services must support legitimate, mission related activities of the county and be consistent with prudent operational, security, and privacy considerations.

v. The ICT Department will take responsibility for all web site content (i.e., "the county web site") and format presentation to reflect the county's mission and in supporting county and departmental objectives.

vi. The County Government has no control over the information or content accessed from the Internet and cannot be held responsible for the content.

#### 4.2.5 Inappropriate use

The following uses of county provided Internet access are not permitted:

i. To access, upload, download, or distribute pornographic or sexually explicit material

ii. Violate any written law

iii. Vandalize or damage the property of any other individual or organization

iv. To invade or abuse the privacy of others

v. Violate copyright or use intellectual material without permission

vi. To use the network and internet for personal financial or commercial gain

vii. To degrade or disrupt network performance

viii. No employee may use county facilities knowingly to download or distribute pirated software or data.

ix. No employee may use the county's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.

### 4.3 Password security

#### 4.3.1 Objective:

Provide guidelines in appropriate management of official passwords to maintain adequate security and integrity of all of the county's ICT systems.

#### 4.3.2 Applies to:

All employees

#### 4.3.3 Key guidelines:

i. The County provides access to network, electronic mail and voice mail resources to its employees in support of the county's mission. Passwords are assigned for access

to each of these resources to authenticate a user's identity, to protect network users, and to provide security.

ii. It is the responsibility of each individual to protect and to keep private any and all passwords issued to him/her by the county.

iii. The ICT Department will establish guidelines for issuing new passwords, deleting passwords as required, and allowing employees to change their passwords.

iv. Although the county strives to manage a secure computing and networking environment, the county cannot guarantee the confidentiality or security of network, e-mail or voice mail passwords from unauthorized disclosure.

v. New employee/user passwords must be requested by the immediate supervisor.

vi. The ICT Department must approve any password change requested by a user's supervisor. Confirmation will be sent to user when a password change is completed at the request of a supervisor.

vii. ICT Support will handle requests from county head of departments made in one of the following ways: viii. Requests may be made in person from 8:00am to 5:00pm Monday-Friday excluding public holidays.

ix. Requests will be submitted via written form.

x. Password account requests must be verified by the employee's immediate supervisor.

xi. The ICT Department will delete all passwords of exiting employees upon notification from Human Resources.

xii. System administrators and users assume the following responsibilities:

xiii. The System administrator must protect confidentiality of user’s password.

xiv. The User must manage passwords according to the Password Guidelines.

xv. The User is responsible for all actions and functions performed by his/her account.

xvi. Suspected password compromise must be reported to ICT Support immediately.

xvii. All passwords must be changed every 3 months.

## 4.4 Intranet usage

### 4.4.1 Objective:

The policy provides guidelines for the appropriate use of the county's Intranet to improve the productivity and effectiveness of our staff and county and to maintain security of our Intranet assets.

### 4.4.2 Applies to:

All employees

### 4.4.3 Key guidelines:

The county Intranet is a proprietary web based source of content, knowledge base, and process tool for our internal employees and managers. Security measures have been established to allow county employees access appropriate sections of the county's Intranet to assist in their efforts in conducting County business

The measures include among others:

i. All full time employees of the county are approved for access to the county Intranet. Part time employees and contracted resources must have management approval for Intranet access.

ii. Intranet security passwords are the responsibility of each individual authorized to access the Intranet. Passwords are not to be shared, swapped, or given out in any form. Keep passwords hidden from view and protect the integrity of your county's employee information. iii. The ICT Department is responsible for setting the goals and objectives for the county's Intranet, determining priorities for adding new content and for maintaining the integrity of the Intranet site.

iv. ICT Department is responsible for defining, creating, and maintaining consistent format for all websites and pages developed for the Intranet regardless of original department source.

v. All content residing on the county's Intranet is the property of the county. vi. Maintenance of the Intranet is an assigned role established by the ICT Department.

vii. The County will provide a central Home Page access that will be the employee's main entry point into the county's Intranet.

Departments may include links in department sites/pages for downloading documents and files in the following formats among others:

- Microsoft Excel
- Microsoft Word
- Microsoft Access
- Microsoft PowerPoint
- Adobe PDF
- Visio
- Images and video files

Downloaded files from the Intranet are considered proprietary information of the county and should be treated as such.

The County's Intranet represents an ongoing reflection of the county and organizations within the county. It is every employee's right and obligation to provide input that constantly improves the accuracy of all content and includes new material for consideration that enhances your experience with the county.

## 4.5 Phone usage

### 4.5.1 Objective:

The policy includes appropriate ways to the use of the county's office phone system in order of maximum productivity and cost effectiveness in usage of this county asset.

### 4.5.2 Applies to:

All employees

### 4.5.3 Key guidelines:

Included in this policy are elaborate guidelines for appropriate use of county office phone systems and cell phones. The two types of phone services have very different issues and require unique guidelines for clarity capabilities are integral parts of the county's assets to help conduct business effectively. Phone systems and equipment are provided to enhance employee capabilities and are not to be construed as assets available for personal use. The following guidelines should be read and understood by all employees.

### 4.5.4 County phone system guidelines

i. The phone systems of the county are assets to assist in conducting county business.

ii. The mobile lines will be determined by the heads of respective departments along with the ICT Department responsible for supporting county PABX telephone systems.

iii. During business hours, all calls should be attended to.

iv. Be courteous and considerate when representing yourself and the county when using county phone services.

## 4.6 Software usage and licensing

### 4.6.1 Objective:

This policy provides guidelines on appropriate use of software products utilizing county equipment and devices.

### 4.6.2 Applies to:

All employees

### 4.6.3 Key guidelines:

This policy is intended to ensure that all county employees understand that no computer software may be loaded onto or used on any computer owned or leased by the county unless the software is the property of or has been licensed by the county.

### 4.6.4 General

a. Software purchased by the county or residing on county owned computers is to be used only within the terms of the license agreement for that software title.

b. To purchase software, users must obtain the approval of their departmental heads who will follow the same procedures used for acquiring other county assets.

c. All approved software shall be purchased through the Purchasing Department.

d. The ICT Department shall be responsible for defining appropriate software titles acceptable for use in the county.

e. Under no circumstances shall third party software applications be loaded onto county owned computer systems without the knowledge of and approval of the ICT Department.

f. Illegal reproduction of software attracts a disciplinary action.

g. It's illegal and against the County policies to use unlicensed or pirated software within the County systems.

### 4.6.5 Compliance

The County will use all software in accordance with its license agreements. Legitimate software will be provided to all users who need it. County users will not make unauthorized copies of software under any circumstances. All users acknowledge that software and its documentation are not owned by the county or an individual, but licensed from the software publisher.

Employees of the county are prohibited from giving county acquired software to anyone who does not have a valid software license for that software title. This shall include but is not limited to clients, vendors, colleagues, and fellow employees.

Any user who determines that there may be a misuse of software within the organization will notify the ICT Department.

### 4.6.6 Registration of software

Software licensed by the county shall not be registered in the name of an individual. When software is delivered, it must first be properly registered with the software publisher via procedures appropriate to that publisher in the name of the county with the job title or department name in which it is used.

After the registration requirements above have been met, the software may be installed in accordance with the policies and procedures of the county. A copy of the license agreement will be filed and maintained by the ICT Department. Once installed, the original installation media should be kept in a safe storage area designated by the ICT Department.

### 4.6.7 Software Audit

ICT Department shall conduct periodic audits of all county owned PCs, including laptops, to ensure the county is in compliance with all software licenses.

Audits will be conducted using an auditing software product.

Software for which there is no supporting registration, license, and/or original installation media will be removed immediately from the user's computer. During these audits, the ICT Department will search for computer viruses and eliminate any thatare found.

The full cooperation of all users is required during software audits and failure to cooperate attracts a disciplinary action.

## 4.7 PC software standards

### 4.7.1 Objective:

Provide guidelines for purchasing and installing software on county PC's

### 4.7.2 Applies to:

All employees

### 4.7.3 Key guidelines:

The purpose for this policy is to explain county software standards and to identify the levels of technical support available to the county employees from the ICT Department. The Software and applications standards to be used in the County are those provided by the ICT Authority and a hard copy is available from the ICT

Department

### 4.7.4 Applicability

The policy applies to all employees of the county requesting the purchase of new computer software and who desire computing support for that application from the ICT support team.

The following software standards have been established to ensure efficient and cost effective usage of county computing assets:

i. To help ensure compatibility between applications and releases

ii. To provide more effective system administration

iii. To assist in the computer planning process and enable the realization of long term goals and the future computing vision

iv. To ensure cost effective purchasing

v. To enable effective tracking of software licenses

vi. To provide cost effective end user software training

vii. To facilitate efficient and effective technical support effort

### 4.7.5 Technical Support

Software support is provided at several levels and is based on whether the software is the county enterprise standard or department specific.

The IT Department shall not provide support for evaluation software, personally purchased software, illegal copies of software, screen savers, shareware, and non-network software that is not included in the standard software list.

Software applications determined by ICT Department to cause computer problems with the county's standard network software will be removed.

### 4.7.6 Role of the ICT Department in the Procurement of Hardware and Software

The Department of ICT will assume the following roles in the procurement process for ICT assets: -

i. Assist departments with evaluating new business software solutions. ii. Act as liaison for departments when dealing with computing vendors.

iii. Recommend and evaluate the tasks/jobs/functions to be accomplished via the new software product. iv. ICT department has the sole mandate of providing hardware and system requirements of any system.

v. Any department wishing to purchase any ICT equipment must make a written request to the Department ICT. The Head of ICT, an ICT officer authorized by the head of ICT shall give written specification document accompanied by a forwarding letter signed by the Head of ICT.

vi. All specifications given by the ICT Department must conform to the ICT Authority standards. A hard copy of the standard is available from the ICT Department whereas a soft copy of the same can be downloaded from http://icta.go.ke/standards/end-user-computing-devices-standard/

vii. ICT staff must be involved during the evaluation of any ICT related tender document to ensure compliance with specifications and ensure reasonably pricing.

viii. All ICT equipment purchased must be inspected by ICT staff and entered in the ICT inventory if the comply with the standards

ix. Install the software as needed.

x. Enforce county hardware and software standards.

**Standard PC Equipment and Software List**

Standard PC hardware and software specifications and configurations are provided by the ICT Department.

## 4.8 Inventory and equipment

### 4.8.1 Objective

Provide management guidelines for managing the use and security of county ICT equipment

### 4.8.2 Applicability

This policy applies to all county employees

### 4.8.3 Key Guidelines

All PC's, equipment, and supplies are purchased for county employee use and productivity. It is the responsibility of all employees to manage the security of county ICT equipment and supplies in order to cost effectively manage the county's expense in these areas.

### 4.8.4 Allocating equipment to employees

i Equipment is assigned to employees based upon their job function.

ii Head of departments should maintain a list of ICT equipment allocated to each employee in the department.

iii All ICT equipment should be tracked.

### 4.8.5 Network access

All PC's are network enabled to access the county's network.

It is the employee's responsibility to maintain appropriate security measures when accessing the network.

### 4.8.6 PC Support

The ICT Department will maintain all ICT equipment owned by the County Government.

Standard configurations are defined to assist in providing responsive support and to assist in troubleshooting your issue or problem. Deviations from the standards are not permitted except in appropriately reviewed and approved situations.

### 4.8.7 Employee training

Basic training for new employees on the use of ICT equipment, accessing the network, and using applications software will be held upon request.

### 4.8.8 Backup procedures

Network data and programs are backed up and archived off site in case of emergency.

An employee shall be responsible for backing up data and software on their assigned PC's.

To protect data and software an employee is required to take one of the following measures:

i Save the data onto external storage, HDD, CD

ii Copy the data to the appropriate network server and store it within employees personal file folder specifically set up for this purpose. This will ensure important data is saved and archived in a normal backup process.

iii An employee shall consult the ICT Department for purposes of backing up large data.

### 4.8.8 Anti-Virus software

The County maintains computer and network Anti-virus software that will automatically scan employees' PC for possible viruses for possible threat.

### 4.8.9 Applications software

Under no circumstances are additional software programs allowed to be loaded onto a PC without the review and approval of the ICT Department. This is a preventive measure to avoid network problems due to viruses and incompatibility issues.

### 4.9 Information security

#### 4.9.1 Objective:

Provide guidelines that protect the data integrity and proprietary nature of the county's information systems.

#### 4.9.2 Applicability

This policy applies to all county employees

#### 4.9.3 Key guidelines:

All Information Security specifications given by the ICT Department must confirm to the ICT Authority standards. A hard copy of the standard is available from the ICT Department. Information security means the protection of the county's data, applications, networks, and computer systems from unauthorized access, alteration, or destruction.

i. The purpose of the information security policy is:

ii. To establish a county-wide approach to information security.

iii. To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of county data, applications, networks and computer systems.

iv. To define mechanisms that protect the reputation of the county and allow the county to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to worldwide networks.

v. To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy.

vi. The county will use a layered approach of overlapping controls, monitoring and authentication to ensure overall security of the county's data, network and system resources.

vii. Security reviews of servers, firewalls, routers and monitoring platforms shall be conducted on a regular basis. These reviews will include monitoring access logs and results of intrusion detection software.

The ICT Department must see to it that:

i. The information security policy is updated on a regular basis and published as appropriate.

ii. Appropriate training is provided to data owners, data custodians, network and system administrators, and users.

iii. Vulnerability and risk assessment tests of external network connections should be conducted on a regular basis.

iv. Training maybe be conducted to ensure that users understand data sensitivity issues, levels of confidentiality, and the mechanisms to protect the data.

### 4.9.4 Data classification

It is essential that all county data be protected. Different types of data require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance.

The County classifies data in three classes as outlined below:

a) **High Risk** - Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure.
Data covered under state legislation or the Data Protection Act, 2012 are in this class.
Payroll, personnel, and financial information are also in this class because of privacy requirements.
The county recognizes that other data may need to be treated as high risk because it would cause severe damage to the county if disclosed or modified.
The data owner should make this determination. It is the data owner's Responsibility to implement the necessary security requirements.

b) **Confidential** – Data that would not expose the county to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. It is the data owner's responsibility to implement the necessary security requirements.

c) **Public** - Information that may be freely disseminated.
All information resources should be categorized and protected according to the requirements set for each classification. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through the county.

Data owners must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to its classification level.

No County owned system or network can have a connection to the Internet without the means to protect the information on those systems consistent with its confidentiality classification.

Data custodians are responsible for creating data repositories and data transfer procedures that protect data in the manner appropriate to its classification.

High risk and confidential data must be encrypted during transmission over insecure channels.

All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.

Backups of data must be handled with the same security precautions as the data itself.

When systems are disposed of, or re-purposed, data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.

### 4.9.5 Access control

There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes. This balance should be recognized and addressed appropriately.

Where possible and financially feasible, more than one person must have full rights to any county owned server storing or transmitting high risk data. The county will have a standard policy that applies to user access rights. This will suffice for most instances.

Data owners or custodians may enact more restrictive policies for end-user access to their data.

Access to the network and servers and systems will be achieved by individual and unique logins, and will require authentication. Authentication includes the use of passwords, smart cards, biometrics, or other recognized forms of authentication.

Users shall not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. All users must secure their username or account, password, and system from unauthorized use.

Empowered accounts, such as administrator, root or supervisor accounts, must be changed frequently, consistent with guidelines established by the ICT Department.

Default passwords on all systems must be changed after installation. All administrator or root accounts must be given a password that conforms to the password selection criteria when a system is installed, rebuilt, or reconfigured.

Logins and passwords should not be coded into programs or queries unless they are encrypted or otherwise secure.

Users are responsible for safe handling and storage of all county authentication devices.

Authentication tokens (such as a Secure ID card) should not be stored with a computer that will be used to access the county's network or system resources.

If an authentication device is lost or stolen, the loss must be immediately reported to the appropriate individual in the issuing unit so that the device can be disabled.

Exiting employee access must be reviewed and adjusted as found necessary. Exiting employees should have their accounts disabled upon exit.

Since there could be delays in reporting changes in user responsibilities, periodic user access reviews should be conducted by the unit security person. Transferred employee access must be reviewed and adjusted as may be necessary.

Monitoring must be implemented on all systems including recording login attempts and failures, successful logins and date and time of logon and log off.

Personnel who have administrative system access should use other less powerful accounts for performing non-administrative tasks.

The Department if ICT will develop a documented procedure for reviewing system logs.

### 4.9.6 Virus prevention

The willful introduction of computer viruses or disruptive/destructive programs into the county environment is prohibited, and violators shall be subject to disciplinary action.

All desktop, servers and workstations systems that connect to the network must be protected with an approved, licensed anti-virus software product that it is kept updated according to the vendor's recommendations.

Where feasible, system or network administrators should inform users when a virus has been detected.

Virus scanning logs must be maintained whenever email is centrally scanned for viruses.

### 4.9.7 Intrusion detection

Intruder detection must be implemented on all servers and workstations. Operating system and application software logging processes must be enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and

monitoring systems must be enabled. Server, firewall, and critical system logs should be reviewed frequently. Where possible, automated review should be enabled and alerts should be transmitted to the administrator when a serious security intrusion is detected. Intrusion tools should be installed where appropriate and checked on a regular basis.

### 4.10 Remote access

#### 4.10.1 Objective:

Providing of guidelines on appropriate use of remote access capabilities to the county's network, business applications, and systems

#### 4.10.2 Applicability

This policy applies to all county employees

#### 4.10.3 Key guidelines:

The purpose of this policy is to define standards for connecting to the county network from a remote location outside the county.

These standards are designed to minimize the potential exposure to the county from damages that may result from unauthorized use of the county resources.

Damages include the loss of sensitive or confidential county data, intellectual property, damage to critical county internal systems, etc.

This policy applies to all the county employees, contractors, vendors and agents with a county owned or personally owned computer or workstation used to connect to the county network.

This policy applies to remote access connections used to do work on behalf of the county, including reading or sending email and viewing Intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, VPN, SSH, cable modems, etc. It is the responsibility of the county employees, contractors, vendors and agents with remote access privileges to the county's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the county network.

#### 4.10.4 Remote connection

Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong password phrases.

Employee user name, login and password shall not be shared to unauthorized personnel.

All ICT equipment that are connected to the county internal networks via remote access technologies must use the most up-to-date anti-virus software.

Third party connections must comply with requirements defined by the ICT Department.

Personal equipment that is used to connect to the county's networks must meet the requirements of the county-owned equipment for remote access.

#### 4.10.5 Enforcement

Any employee found to have violated the remote access policy shall be subjected to disciplinary action.

The ICT Department is responsible for monitoring remote access and addressing inappropriate use of remote access privileges.

### 4.11 Privacy

#### 4.11.1 Objective:

Provide guidelines on appropriate management of employee and client privacy

#### 4.11.2 Applicability

This policy applies to all county employees

#### 4.11.3 Key Guidelines

This document describes the county's policy regarding the collection, use, storage, disclosure of and access to personal information in relation to the personal privacy of past and present staff, clients and other stakeholders of the county.

### 4.11.4 Handling personal information

The following policy principles apply to the collection, use, storage, disclosure of and access to personal information:

i. The collection and use of personal information must relate directly to legitimate purposes of the county.

ii. Individuals must be informed of the purpose for which personal information is obtained.

iii. The County will take all reasonable measures to ensure that the personal information it receives and holds is up to date.

iv. The County will take all reasonable measures to store personal information securely.

v. Individuals are entitled to have access to their own records, unless the disclosure of that information is unauthorized.

vi. Third party access to personal information may only be granted in accordance with the procedures made pursuant to this policy

This Policy does not apply to personal information that is:

i. In a publication available to the public

ii. Kept in a library, art gallery or museum for reference, study or exhibition

iii. A public record under the control of the keeper of public records that is available for public inspection

iv. The ICT department shall be responsible for ensuring compliance with the policy

v. This policy applies to all organizational areas and is binding on all employees.

### 4.11.5 Personal Information

Refers to Information obtained by the county which pertains to an individual's characteristics or affairs.

The personal information can be recorded in any format - for example, in writing, online, digitally or by electronic means.

#### 4.11.6 Complaints

Any person, whether or not an employee of the county, who on reasonable grounds believes that a breach of this policy has occurred within the county, may direct them complains to the County ICT Department for further actions. The ICT Department shall investigate complaints as expeditiously as practicable and shall provide a written copy of the findings of fact and recommendations made to both the county and to the individual filing the complaint.

The department of Human Resources will determine what action will be taken on any recommendation contained in the findings of the Privacy Officer

### 4.12 Service level agreements

#### 4.12.1 Objective:

This policy provides guidelines on how the ICT Department shall enter into service level agreements with Service suppliers.

#### 4.12.2 Applies to:

Suppliers and the Head of ICT department

#### 4.12.3 Key guidelines:

i. Service Level Agreements will be maintained between the ICT Department and the service suppliers
ii. These Service Level Agreements will be reviewed on a regular basis in order to provide flexibility in light of changing needs.
iii. Demand for the IT Department's products and services is likely to increase over time and there should be clear agreement over the extent and type of information to be provided and over services to be carried out in respect to supporting the User. iv. Part of the function of a Service Level Agreement is to manage expectations of both sides of the agreement.

### 4.13 Network Installations and Administration

#### 4.13.1 Objective

This policy provides guidelines on how the ICT Department shall come up with the network specifications, administer and maintain the Network.

#### 4.13.2 Applicability

The head of the ICT department and all staff in the ICT Department

#### 4.13.3 Key Guidelines

i. All network specifications are to be requested to Head of ICT in writing.
ii. All specifications shall be given in writing and must comply with the ICT Authority standards. A hard copy of the standard is available from the ICT Department. The soft copy of the standard is available at http://icta.go.ke/standards/ict-networks-standard/
iii. All Network inspections shall be done by the department of ICT to confirm they comply with the requirements.

## 5. ACTORS / STAKEHOLDERS ROLES AND OBLIGATIONS

### 5.1 The County Government

The county government plays a major role in financing of the ICT board so as to achieve objectives of this policy. These roles include:

- Allocating funds to the ICT department.
- Hiring of ICT Staff.
- Creating an enabling environment for the ICT Department to partner with private institution
- Ensure coordination with other departments in the implementation and adherence to this policy.

### 5.2 The County Assembly

The county assembly with its mandate shall legislate on laws regulating ICT in the county. The county assembly will further consider and approve budgetary allocations to the ICT department in accordance to the advisory to allocate 5% of the county budget.

### 5.3 ICT Steering/Governance Committee

The County executive shall establish an ICT steering/governance committee whose functions shall be:

- Define the mission and goals of ICT resources to align with the strategic direction of the county;
- Authorize and direct the development of the strategic and operational plans for ICT resources;
- Ensure that ICT resources strategic and operational plan align with the county's directions;
- Review and approve business cases to ensure that ICT resources are optimized;
- Determine and monitor organization security policies on an ongoing basis to ensure that they continue to remain relevant and complete;
- Ensure policy exists to establish authority, accountability, and responsibility relating to information and technology;
- Ensure the County has a sustainable, institutional funding model for ICT infrastructure and services;

- Ensure existing and emerging technologies that enable the pursuit excellent public service delivery and reporting are broadly available people of Machakos County;
- Ensure the county has an effective ICT and information security framework with appropriate ICT controls;
- Support requests for major ICT initiatives where appropriate, and provide advice for allocating resources for such initiatives; and
- Provide direction to prevent, where appropriate, unnecessary redundancy or non-sustainable service implementations and their resulting inefficiencies and risks.

### 5.4 The ICT Department

The main implementer of this policy shall be the ICT department in conjunction with other departments.

The roles of ICT include:

- To setup and design the ICT infrastructure
- Advise on the appropriate specifications for software and ICT equipment to meet the ICT needs of the county government.
- To supervise the compliance to this policy.
- Offers ICT system user training to maximize the use of ICT.
- Support and regulate maintenance of the ICT equipment
- Setup access controls and ICT security systems to ensure the safety of the county assets.
- Setup data storage, backup and recovery centers to ensure data security and availability.

### 5.5 ICT Government Agencies

This are organizations in the composition of the government responsible for administration and oversight of ICT and to ensure easy, convenient and efficient access to government systems. The roles of ICT Government agencies include:

- Providing network infrastructure for connectivity between the county, other counties and the national government.
- Providing infrastructure that is related to ICT such as; fiber optic, internet, WIFI hotspots, CCTV cameras that increase security, roads, railway, electricity, that facilitate access to rural and remote areas.
- To ensure that ICT plans and strategies are consistent at all levels of government.

- To create a conducive environment for organizations and investors that are desirous of collaborating with the County Government on ICT.

## 6. TARGETED AUDIENCE ROLES AND OBLIGATIONS

The target audience of this ICT policy include different groups of stakeholders who will take part in the implementation, monitoring and evaluation:

### 6.1 System users/Employees

These are the people who interact with ICT systems in performance of their daily duties. To achieve the objectives of this policy the users will need to cooperate with the ICT department by;

- Allowing access to assigned ICT equipment for audit and configuration.
- Providing information on any violation of this policy
- Provide feedback on performance of ICT systems to help improve usability

### 6.2 The General Public

The ICT department will setup iHub centers with which is fully equipped with the necessary equipment's and trained staffs according to this policy to ensure availability of ICT to the public at a reasonable cost. The public shall be required to use the provided ICT equipment responsibly and in accordance with the set guidelines

## 7. MONITORING AND EVALUATION

### 7.1 Definition

Monitoring and evaluation (M&E) are two distinct but comprehensive processes that are, usually reinforce each other, in general, M&E is designed to monitor the impact of a policy, or progress of programme activities against the overall goals, objectives and targets. M&E also assess the outcome relevance of an activity, and the impact of a programme, or effectiveness of a policy, as well as its efficiency and sustainability

The implementation of the County ICT Policy shall be monitored and evaluated for effectiveness and responsiveness in meeting intended goals and objectives.

Monitoring will be done annually or as may be determined by the stakeholders.

Evaluation shall be conducted every three years to measure impact.

A compressive M&E activity shall be the basis for*:* -

1. Guiding decision making in the ICT Department and stakeholders, by characterizing the implication of progress (or lack of it) being made by the ICT Department in the implementation of the ICT Policy.
2. Guiding implementation of ICT policy by providing information on progress and results.
3. Providing a unified approach to monitoring progress made by the ICT Department and all stakeholders in the implementation of ICT Policy.

### 7.2 M&E Implementation Plan

- Collecting the data

  A team to be agreed upon by the stakeholders will undertake field visits. They will state what the team is to check and observe in the implementation of the ICT policy objectives.

  - Stakeholders meeting will be held to review the progress made. This include but not limited to; the ICT Department will conduct periodic audits of all county owned PCs, including laptops, to ensure the county is in compliance with all software licenses.

- Situation analysis and progress reports will have produced on a quarterly basis with a format agreed upon by all the stakeholders. These reports will serve as a checklist for

the ICT policy objectives accomplished, what has not been accomplished and the reasons for not accomplishing the activities.

### 7.3 Disseminating the reports of M&E

The reports prepared from these above will be forwarded to the ICT Department and all stakeholders as necessary and feedbacks will be given so that action can be taken. The policy shall reviewed frequently based line with emerging global trends in technology.