

# **COUNTY GOVERNMENT OF KIRINYAGA**



## **OFFICE OF THE COUNTY SECRETARY**

### **KIRINYAGA COUNTY ICT POLICY**

## **Approval**

This ICT Policy document shall be reviewed by Kirinyaga County cabinet resolution.

The effective date shall be from the date of approval.

## Acronyms

<b>CD</b>	Compact Disk
<b>DICT</b>	Director ICT
<b>DDICT</b>	Deputy Director ICT
<b>DRS</b>	Disaster Recovery Site
<b>DVD</b>	Digital Video Disk
<b>ICT</b>	Information and Communication Technology
<b>ISO</b>	International Organization of Standards
<b>IT</b>	Information Technology
<b>LAN</b>	Local Area Network
<b>PABX</b>	Private Automatic Branch Exchange
<b>PC</b>	Personal Computers
<b>SAN</b>	Storage Area Network
<b>SLA</b>	Service Level Agreement
<b>WAN</b>	Wide Area Network

## Table of Contents

Approval .....	2
1.0 Introduction .....	5
2.0 The ICT Mandate.....	5
3.0 Objectives .....	6
4.0 Scope.....	6
5.0 ICT Facilities Usage .....	8
6.0 ICT Security .....	8
7.0 Network Access & Permissions .....	9
8.0 Website(s).....	10
9.0 ICT Equipment Maintenance. ....	10
10.0 Email Usage.....	11
11.0 Internal ICT Support .....	11
12.0 The Internet .....	12
13.0 Out-Sourced ICT services .....	13
14.0 ICT Staffing.....	13
15.0 Acquisition and Disposal of ICT Facilities .....	13
16.0 Backup & Disaster Recovery .....	14
17.0 Printers, Telephone Lines, Fax, Scanners and Copiers.....	15
18.0 ICT Training .....	15
19.0 Online Subscriptions for Kirinyaga County products .....	16
20.0 Enforcement and Control .....	16
21.0 Privacy and Confidentiality.....	17
22.0 Revision.....	17
22 References.....	17

## **1.0 Introduction**

The ICT department is a structure within the County Government of Kirinyaga.

The ICT Department will provide ICT services for enhanced efficiency. In provision of such services, the Department proposes that adequate resources are provided to implement a reliable and appropriate IT infrastructure, inclusive of reliable internet connection in all county offices. It is thus imperative that acquisition and usage of such facilities requires to be governed by an organization wide ICT policy.

The ICT policy has been developed taking into account

- 1) National Policy on Information and Communication Technology (ICT); GoK, 2007.
- 2) ICT Standards and Guidelines. Directorate of E-Government. Kenya (2011).
- 3) ICT Policy Formulation and E-Strategy Development. A Comprehensive Guidebook. Asia-Pacific Development information Programme, UNDP, 2011.

## **2.0 The ICT Mandate**

The ICT department is mandated by the County Government of Kirinyaga to;

- a) To develop & promote competitive ICT infrastructure in the county.
- b) Appreciate, disseminate and implement the Kirinyaga County e-Government strategy.
- c) Develop ICT Strategic Objectives, work and project plans for the county.
- d) Contextualize, disseminate and implement the County e-Government ICT policy.
- e) Implement ICT projects based on the County e-Government strategy.
- f) Provide technical and operational support for systems and infrastructure. Including networks, websites, email systems, databases and applications.
- g) Provide ICT technical user support and training.

- h) Identify ways in which the Kirinyaga County can more effectively and efficiently deliver services to the citizens using ICT and propose appropriate interventions.
- i) Monitor, coordinate and advise on issues pertaining to electronic business, telecommunications and technology.
- j) Participate in the development, analysis and evaluation of County wide technology issues, policies and legislations.

### **3.0 Objectives**

This policy seeks to;

- a) Ensure provision of adequate and reliable information systems in the County
- b) Provide guidelines on the usage of ICT software, hardware and services in the County
- c) Ensure information security of the County systems and data
- d) Promote efficient utilization of information systems within the County
- e) Ensure application of best practices and standards
- f) Promote spirit of awareness, co-operation, trust and consideration for others.

### **4.0 Scope**

This ICT policy covers all IT facilities, hardware, software, and service, provided by the County. These are:

- a) Facilities
  - i. Data processing center
  - ii. Server room(s)
  - iii. ICT maintenance room
  - iv. Data Recovery Site(s) (DRS)
  - v. ICT facilities installed at Kirinyaga County Branches such as Sub-County Offices and other county offices.
- b) Services
  - i. Provision of guidance and expertise training on ICT
  - ii. ICT support in software, hardware and any other computing infrastructure

- c) Technical support to Hardware such as;
  - i. PCs
  - ii. I-pads
  - iii. Laptops
  - iv. Printers
  - v. Photocopiers
  - vi. Scanners
  - vii. Servers
  - viii. Network routers and switches
  - ix. Power backup equipment (e.g. Uninterruptable Power Backup -UPS)
  - x. Display devices e.g Projectors
  - xi. Network Devices
  - xii. Cameras (Digital and Camcorders)
  - xiii. PDAs, Smartphone's and other Mobile Computing Devices
  - xiv. Diskettes/CDs/DVDs
  - xv. Flash-disks/external hard-disks
  - xvi. PABXs, Telephone heads, fax and photocopiers
  - xvii. All other ICT related hardware
- d) Software
  - i. Network operating systems
  - ii. PC operating systems
  - iii. Application software
  - iv. Utility software
  - v. Custom made Systems/Software's

e) County Offices

The policy covers all county offices and branches. These will be supported from the county headquarters.

f) Gender

The policy caters for persons of all genders without discrimination in line with the national policy on gender.

g) Disability

The policy caters for persons with disabilities in that the Finance Ministry will endeavor to provide specialized equipment and services to disabled persons so as to enable them make maximum use of ICT services.

## **5.0 ICT Facilities Usage**

- a) All ICT facilities owned by the Kirinyaga County will be issued for staff official use through the Procurement and issuance procedures.
- b) The ICT Department will be the custodian of ICT systems including software, and hardware as a measure to facilitate standardization. Thus, officers will be availed hardware, software and system relevant to their work requirements.
- c) Staff shall take maximum care of such facilities and ensure responsible usage and custody of equipment.
- d) Sharing of Kirinyaga County ICT resources will be encouraged so as to enhance their optimal utilization.
- e) Users shall not relocate, repair, reconfigure, modify Kirinyaga County ICT equipment or attach external devices other than for data storage to such equipment without the authority from ICT department. The devices should be scanned for any malware before being used.
- f) Kirinyaga County shall authorize Staff to use external disks only for the purpose of storing official information. such external disks must be scanned for viruses and other harmful software.
- g) Personal software, hardware or systems shall not be used within Kirinyaga County LAN.
- h) Food or drinks shall not be allowed on or near any ICT equipment.

## **6.0 ICT Security**

- a) All Kirinyaga County systems and information shall be effectively protected against unauthorized access.
- b) The ICT Directorate shall provide network service to staff to transmit data to requesters and store data files in an authenticated central server.



- c) Users within same directorate/working group will be given access level that allows them access to their files/folders.
- d) For traceability and identification, all hardware shall be coded and included in the Kirinyaga County asset register. This shall include any hardware bought /donated to Kirinyaga County by external agencies.
- e) ICT devices are susceptible to theft and unauthorized access, thus, strong security measure to safeguard them shall be provided.
- f) Portable or laptop computers shall not be left unattended in public places, and shall be carried as hand luggage for security.
- g) Portable computing equipment for short term lending shall be stored in secure lockable cabinets.
- h) An updated register of all ICT equipment shall be maintained. This will also include Equipment loaned out to authorized personnel.
- i) All data storage media shall be stored in secure environments that meet manufacturer's specifications for temperature and humidity.
- j) Hard copies of systems documentation shall be physically secured in filing cabinets when not in use.
- k) It is the responsibility of respective users of any non LAN-connected and official computing equipment (especially laptops/notebooks) to arrange with the ICT support for installation of antivirus software and to perform periodic (at most every fortnight) updates to the antivirus.
- l) All ICT hardware or software will not be taken off-site from Kirinyaga County offices, for servicing /or upgrading without written authority from the Department.

## **7.0 Network Access & Permissions**

- a) Each user will have only one personal identification code (User ID/user name and password) with necessary access levels and privileges.
- b) User IDs will be consistent in structure i.e. the first letter of the firstname and last name, all in lower cases (ignoring middle names). If this combination conflicts with another user, then the first letter of secondname will be used as the second letter of the user ID. If the officer does not have other names, then letter 'a' through 'z' will be used so that user ID is unique within Kirinyaga County access systems.

- c) All devices will require access credentials (user ID and password) to be accessed over the network. Guidelines on structure of user IDs and passwords will be provided by ICT Directorate.
- d) Users will be responsible for the confidentiality of their access credentials and prevention of any unauthorized access to ICT equipment. Any attempt to use other Staff users' credentials to gain access to network resources is strictly disallowed. Any account found to be compromised or shared shall be discontinued and a new one issued where necessary.
- e) Only authorized personnel are allowed access to ICT resources.
- f) Authorized ICT Staff or any other staff with permission is authorized to gain access to a user account and folders if that account is suspected to have breached systems security or is in violation of this policy.
- g) The ICT Department shall enforce standardization of systems and network configuration, including directory structures, to simplify network management.

## **8.0 Website(s)**

- a) The ICT department shall ensure that the Kirinyaga Website(s) is kept in an updated status at all times. By use of the latest technology, the website shall be maintained in a user friendly and accessible state.
- b) All requests for changes on the website shall be subject to the approval of the Kirinyaga website committee.
- c) The ICT Department shall ensure that the website is always available to the public.
- d) All the staff shall be provided with official standardized domain e-mail addresses.

## **9.0 ICT Equipment Maintenance.**

- a) The Department shall ensure that all ICT equipment is kept in proper working condition at all times.
- b) All ICT equipment shall be maintained in accordance with the procedure for ICT equipment maintenance.

- c) Where ICT equipment are located within locked premises, the custodians of such places should allow ICT officers access the equipment.
- d) Periodic Preventative maintenance procedures will be undertaken to ensure ICT equipment are working optimally.
- e) In areas where the department has no adequate internal capacity, maintenance contracts will be entered into with service providers.

## **10.0 Email Usage**

- a) Staff shall be issued with official standardized e-mail addresses as outlined in section 8.0 above.
- b) All official email communications shall be through official email addresses. Department will ensure that mail service is available to staff always.
- c) The Kirinyaga's Intranet will be used to communicate all relatively static information (e.g. policies, procedures, briefing documents, reference material and other standing information).
- d) Email users shall avoid broadcast communication (i.e. send to large groups of people using email aliases) unless where absolutely necessary. One must always ensure proper audience segregation is used before sending an email.
- e) Kirinyaga mail service shall not be used to broadcast other unofficial information or requests (e.g. Information or opinions on political matters, social matters, and personal requests for information etc.)
- f) Emails with attachments greater than 10MB will require authorization from department. This will remove unnecessary load on the network and the mail server so as to guarantee equitable bandwidth sharing by all staff.
- g) Emails with suspicious content, attachments or web links should be reported to the ICT department for further action.

## **11.0 Internal ICT Support**

- a) While Kirinyaga County will strive to provide ICT support services, officers assigned to hardware must ensure they are not exposed to risks that can cause their damage.

- b) ICT officers will be available to offer technical support on any software or hardware upon users' requests.
- c) Where applicable, equipment to be used out of office shall be accompanied by an ICT Technician to ensure proper packaging, offloading and installation at destination.

## **12.0 The Internet**

- a) All connections to the Internet within Kirinyaga County offices shall be implemented through the Kirinyaga Internet connections via a firewall.
- b) To protect Kirinyaga systems from Internet attacks or denial of service by Internet malware, all software downloads shall be authorized by ICT Department. Such a download will be passed on to the requester only if it passes the ICT security tests and if it is permitted for free use by its manufacturers.
- c) No copyright material shall be downloaded from the internet or utilized in breach of its license agreement.
- d) Internet services shall be provided only through the Kirinyaga County Internet connection or Kirinyaga USB modems or any other approved gadgets.
- e) To optimize internet bandwidth usage, County's network shall not be used to stream music and video as these lead to deprivation of the same capacity to legitimate users during normal working hours except, where such permission is granted in writing.
- f) Kirinyaga internet and network resources shall not be used to access or transfer any material containing:
  - i. Derogatory remarks based on race, religion, gender, physical disability or sexual preference.
  - ii. Images or references that may be considered to be offensive or in breach of any law or regulation.

### **13.0 Out-Sourced ICT services**

- a) The County shall out-source ICT Equipment /or services whenever such capacity lacks in the County with approval from an authorized department.
- b) All out-sourced ICT equipment and services shall be supervised by ICT Department in accordance to the Service Level Agreements (SLAs) that are signed between the user i.e. ICT department and the service provider.

### **14.0 ICT Staffing**

The Department shall endeavor to

- a) Equip and maintain adequate and highly skilled ICT personnel for guaranteed minimum acceptable ICT service level.
- b) The ICT function will be executed through the ICT Department headed by an ICT Director.
- c) All ICT Projects will be coordinated and supervised by the Director ICT.

### **15.0 Acquisition and Disposal of ICT Facilities**

- a) Acquisition of ICT Facilities
  - i. Acquisition of ICT facilities shall be guided by the Public Procurement Procedures and Guidelines in the Public Procurement and Disposal Act (PPAD), 2015, Public Procurement and Disposal Regulations(PPADR)2020, Best Practices and the Kirinyaga County Procurement Manual or any other current act & regulation formulated by the government of Kenya.
  - ii. Where funds donated from external sources, the respective donor conditions, terms, agreements or memoranda of understanding shall apply.
  - iii. All User requests for acquisition of items of ICT nature shall be channeled through the ICT Director who will confirm lack or availability of such items. If not available, ICT Director or any other ICT staff will prepare specifications in consultation with the

requesting department and forward the request to the Chief Officer for approval.

- iv. In order to minimize the costs, Kirinyaga County will standardize software and hardware to be used within the County with advice from authorized Directorate e.g. ICT Authority
- v. All departments will forward to ICT department their software and systems needs who will offer technical guidance and support in facilitating the acquisition process.
- vi. ICT goods, related services and/or works once acquired will be received by the County Inspection and Acceptance Committee in line with The Public Procurement and Assets Disposal Act (PPAD), 2015 and Public Procurement and Disposal Regulations (PPDR), 2020 framework or any other current act & regulation formulated by the government of Kenya.

b) Disposal

- i. ICT department shall identify hardware and software to be disposed and in consultation with the Chief Officer and CEC in charge of Finance, liaise with Procurement Department for assessment leading to disposal as per PPAD, 2020.

## **16.0 Backup & Disaster Recovery**

- a) Kirinyaga information resources such as data, business contacts, emails, text documents, presentations, contracts, accounts and other valuable information shall be safely preserved in a recoverable state.
- b) ICT Department will maintain consistent automated backup mechanisms to preserve Kirinyaga County data in a distributed Storage Area Network (SAN) and at a DRS in order ensure data recovery in the event of accidental loss.
- c) All Kirinyaga data shall be saved in organized shared folders in allocated branch servers from where they will be backed up in SAN and Disaster Recovery Site (DRS) through synchronized mechanism in addition

to tapes or external drives in accordance with the Kirinyaga County Backup Plan.

- d) Network and server administrators will ensure data is copied to these allocated servers and in all other backup destinations.
- e) It is the responsibility of the respective users of any non LAN-connected computing equipment (including laptops/notebooks) to arrange with the server administrator for the transfer of official data from these non LAN-connected equipment to the relevant server folders every day where practical.
- f) Any unofficial files shall not be allowed on Kirinyaga County Servers.
- g) Only authorized personnel will be able to visit off-site DRS.
- h) To implement an ICT seamless backup service, all officers connected Kirinyaga LAN shall login to centralized authentication servers. Officers working from remote locations will be required to dock to the Kirinyaga network to back up official data.

## **17.0 Printers, Telephone Lines, Fax, Scanners and Copiers**

- a) Kirinyaga County Staff are expected to use the above peripheral devices responsibly. Irresponsible or usage of these facilities for personal gain is prohibited, and may lead to denial of the service and/or surcharge.
- b) Where possible, users are required to print on both sides of the paper. ICT support team will give guidance on how various printers are able to print both sides.
- c) Printers will be configured to be shared by many users and placed in secured open offices where possible.
- d) Unofficial calls and fax will be charged on the user.
- e) An electronic document scanner shall be used to minimize usage of fax machines, saved in suitable formats and emailed to recipients.

## **18.0 ICT Training**

- a) The department shall identify ICT training needs for officers in the department and forward to the Office of The County Secretary for recommendations and factoring in the county training plan.

- b) Members of staff shall undergo continuous ICT training for them to effectively use the ICT resources and services and keep at pace with changing ICT technologies.
- c) ICT Training shall be done internally or in conjunction with other government entities such as ICT Authority or any other training institution as may be deemed eligible to offer specialized training in accordance with the procurement regulations.

## **19.0 Online Subscriptions for Kirinyaga County products**

- a) Online subscriptions for Kirinyaga County products shall be done via the Kirinyaga County official web portal. Such subscription shall be handled by the authorized staff as per the County's Data Access and Dissemination Policy.
- b) Official payments to such online subscriptions shall follow the Finance Manual.

## **20.0 Enforcement and Control**

- a) Deliberate breach of this policy statement may lead to disciplinary measures in accordance with Kirinyaga County Human Resource Manual. These may include but not limited to the offender being denied access to computing facilities or surcharge for the loss or abuse of ICT facility or service.
- b) Whenever surcharge is imposed on negligence as noted in (a) above, due process will be followed in imposing the surcharge.
- c) Unauthorized access to information, facility or computer (including workstations and PCs), over network or to modify its contents is strictly forbidden.
- d) Officers within Kirinyaga County Government network shall not write, publish, browse, bookmark, access or download obscene, pornographic or pedophilia materials.
- e) All hardware, software and /or systems in use in Kirinyaga County Government offices shall be licensed. Any officer using unlicensed products shall bear legal consequences for the product as per 'the Copyright Act, 2001'.



## **21.0 Privacy and Confidentiality**

- a) The ICT department shall guarantee right to privacy and confidentiality of individual staff information while discharging ICT services.
- b) Information/services/resources available within ICT facilities will not be used to monitor the activity of individual staff in anyway (e.g. to monitor their working activity, working time, files accessed, internet sites accessed, reading of their email or private files etc.) without their prior knowledge. Without limitation to this provision, the following shall be excluded:
  - i. In the case of a specific allegation of misconduct, the Management may authorize access to such information or denial of service while the staff is under investigation.
  - ii. Where the ICT Department or any other section cannot avoid accessing such information whilst administering, resolving ICT systems problems or in their day to day work activities.

## **22.0 Revision**

This policy shall be revised every three years or as and when need arises under the authority of the Chief Officer in charge of ICT to keep in tandem with changes in technology, statutory regulations or for any other purposes as may be advised from time to time by authorized National ICT bodies.

## **23.0 References**

- 1). National Policy on Information and Communication Technology (ICT); GoK, 2007.
- 2). ICT Standards and Guidelines. Directorate of E-Government. Kenya (2011).
- 3). ICT Policy Formulation and E-Strategy Development. A Comprehensive Guidebook. Asia-Pacific Development information Programme, UNDP, 2011.