KENYA FORESTRY COLLEGE

INFORMATION COMMUNICATION TECHNOLOGY (ICT) USE POLICY

DATE: 23RD SEPTEMBER, 2020

Table of Contents

i. ABBREVIATIONS AND ACRONYMS

CD – Compact disk

ERP- Enterprise resource planning

ICT – Information communication Technology

ICTA- Information communication Technology Authority

IEEE-Institute of Electrical and Electronics Engineers

ISO- International Organization for standardization

GIS - Geographic Information System

HR-Human Resource

KFC-Kenya Forestry College

KFS- Kenya Forest Service

LAN – Local Area Network

LCD - Liquid Crystal Display

DLE - Digital Learning Environment

PC - Personal Computer

UPS- Uninterrupted Power Supply

WAN – Wide Area Network

ii. DEFINITIONS

For the purpose of this policy unless the context otherwise requires the following are explained as given;

1. **Accessories** - Keyboard, mouse, data cables, CD-Rom, adapters
2. **Data center**- Facility used to house computer systems/servers and associated components.
3. **ICT equipment/Hardware**- Servers, desktops, laptops, printers, scanners, photocopiers, external disks, LCD projectors, CD-Rom, UPS, digital cameras, network devices (routers, switches, hub etc), mobile devices (Ipads, tablets, smart phones)
4. **ICT resources** - ICT equipment, Accessories and installed software including Infrastructure such as ICT networks and application systems namely e-mail, ERP (Oracle Financials system), GIS systems, various Microsoft Office packages (Word, Excel, project, Access, PowerPoint), Internet and any other authorized/licensed software in use at the service.
5. **License**- User right to use the software in the licensed environment
6. **Software**-Operating systems (Windows, Linux/Unix), ERP application, In-house developed system, off-the shelf systems, Antivirus etc.
7. **Virtual Private Networks (VPN)** - Extends network across the Internet enabling users to send and receive data across shared or public networks as if they are directly connected to the KFS network, while ensuring security and applicable policies are observed.
8. **Wireless LAN** also known as Hotspot or Wi-Fi are networks rolled out using radio waves to provide mobile network access as defined under IEEE 802.11 protocol.
9. **ICT networks** - Two or more computer systems linked together
10. **Wireless device** - Communication device that does not require a physical wire to relay information
11. **System backup** - process in which the state, files and data of a computer system are duplicated to be used as a backup or data substitute when the primary system data is corrupted, deleted or lost.
12. **Business Continuity Plan (BCP)** - Creating systems of prevention and recovery to deal with potential threats to the Service.
13. **Information systems** - Organized system for the collection, organization, storage and communication of information.

iii. RELATED/RELEVANT PROCEDURES, POLICIES AND LAWS

1. ICTA documents - ICT Security and Usage Policy
2. KFS ICT Operational Procedures
3. KFS Strategic Plan
4. KFC Strategic Plan
5. Relevant laws
    a. The Copyright, Designs and Patents Act 1988
    b. The Data Protection Act, 1998
    c. The Human Rights Act, 1998
    d. The Computer Misuse Act, 1990
    e. The Regulation of Investigatory Powers Act, 2000
    f. The Freedom of Information Act, 2000
    g. The Electronic Communications Act, 2000
    h. The Digital Economy Act, 2010
    i. Kenya Communications Act
    j. Access to information Act, 2015
    k. Personal information protection Act, 2010
    l. Forests conservation and management Act, 2016
    m. NEMA e-waste guidelines 2010
    n. Public Procurement and Asset Disposal Act Revised Edition 2016
    o. The Copyright, Designs and Patents Act 1988
    p. The Digital Economy Act 2010

DOCUMENT REVISION HISTORY

Version	**Date**	**Author/s**	**Revision Notes**
1.0	August 2020	Principal KFC/Head of ICT in KFS	Revised draft
1.1	September 2020	KFC/KFS	Approved Draft
1.2			
1.3			
1.4			
1.5			
1.6			

1. INTRODUCTION:

The Kenya Forest Service is a corporate body that was established under the Forest Conservation and Management Act, 2016 (henceforth referred to as the Act). “To enhance development, conservation and management of Kenya’s forest resources base in all public forests and assist county governments to develop and manage forest resources on community and private lands for the equitable benefit of present and future generations”.

To effectively implement this mandate and to also build the human capital with skills required within the sub sector training is an important activity that must be in place. In furtherance of this Service administers the Kenya Forestry College (KFC) at its training arm.

KFC is a technical training institution legally established through section 17 of the Act. It is the entity that provides for the promotion forestry education and training by the Kenya Forest Service.

The College is duly registered with the Technical and Vocational Education and training Authority (TVETA).

The mandate of the College is provide quality training education and training for sustainable management and utilization of forests and allied natural resources. It has the following vision and mission.

Vision:

The College’s vision is to be an international Centre of excellence for applied education in sustainable management of forests and allied resources.

Mission:

Development and dissemination of best practices in the management of forests and allied resources through quality teaching, research and outreach is the Mission of the College.

ICT is an important tool in conservation and management of forest resource in Kenya and therefore there is need to provide guidelines for use of ICT in achieving the above mandate.

KFC has adopted the use of ICT in its day to day operations which brings with it various benefits and challenges. Whereas the benefits cannot be gainsaid, the challenges range from limited resources or ICT investment, complexity of systems, lengthy learning curves, security, dynamic nature of ICT and legal compliance.

Moreover ICT professionals are called upon to make decisions on whom to grant or deny access to ICT resources, what defines proper use of ICT, type of training due to change of technology. Due to lack of proper policy guidelines, such decisions often lack consistency across the organization and are often ineffective and costly.

This policy document therefore will provide the framework for best practice, enhance proper use and safeguard the integrity of the implemented ICT systems at KFC.

This policy document will serve as the reference on ICT guidelines for all ICT users. Additional policies may be issued from time to time to support this policy.

2. RATIONALE:

Some of the major reasons for formulating this ICT policy are:

a. Due to rapidly changing technologies, planning becomes increasingly important in order to avoid incompatibility and inaccessibility.
b. To address the severe scarcity of adequately trained and experienced analysts, software engineers, systems and network managers, coupled with their long training cycles constrains ICT developments.
c. To tackle the scarcity of financial and managerial resources.
d. The development of academic programs, courses, services, research programs, educational technological activities, policies and methods as well as the growth of the number of trainees and faculty will depend on the availability of ICT services and systems.
e. To integrate the College ICT policy to be in line with the KFS and National ICT Policy.

3.0 AIM OF THE ICT POLICY:

To support the strategic vision of the Kenya Forest Service and to enhance performance of Kenya Forestry College by improving operational efficiency and exchange of information so as to maintain a competitive edge.

3.1 PURPOSE AND OBJECTIVES:

The purpose of this Policy is to outline the guidelines for acceptable use of ICT resources in KFC. These guidelines will ensure that these resources are available to all authorized members of staff on timely basis to facilitate their business operations. All KFC's ICT resources are the property of the Kenya Forest Service.

The objectives of this policy are to;

a. Enhance compliance with the existing Kenyan laws.
b. Serve as a guideline to KFC staff working in the College, trainees and the public on the best ICT practice in usage of ICT resources.
c. Provide guidance in the development, use and maintenance of reliable, secure and cost

effective ICT systems.

d. To provide guidance for the acceptable use of ICT Resources at the College.

e. To outline development, implementation and sustainability of ICT in the College.

f. To promote efficient and effective usage and operations of ICT based systems in the College.

g. To ensure users have proper awareness and concern for the security of ICT resources and adequate appreciation of their responsibilities during its use.

h. To ensure users are aware of their legal obligations when using ICT resources.

a. Guide the handling of organizational information within the Service by ensuring compliance with applicable statutes, regulations, and mandates for the management of information resources and thereby establish prudent practices.

b. Guide the process of enhancing utilization of ICT resources through training and development.

c. Improve consistency of decision making.

d. Provide cost effectively information and communication technology facilities, services and automation.

e. Provide guidance in the development, use and maintenance of reliable, secure and cost effective ICT systems.

f. Guide the handling of organizational information within the College by ensuring compliance with applicable statutes, regulations, and mandates for the management of information resources and thereby establish prudent practices.

g. Uphold the integrity and image of the Service and College by ensuring that the content of it’s websites is accurate, consistent and up-to-date.

h. Outline the guidelines that ensure ICT resources are serviceable.

i. Help people to adapt to new circumstances and provide tools and models to respond rationally to challenges posed by ICT.

j. Promoting information sharing, transparency and accountability and reduced bureaucracy in operations

k. Guide the process of enhancing utilization of ICT resources through training and development.

l. Improve consistency of decision making.

m. Identify priority areas for ICT development.

n. Improve on customer satisfaction.

o. Help save resources.

4. APPLICABILITY AND COMPLIANCE:

This policy applies to all KFC staff, trainees and third party persons/organizations accessing, developing, implementing and/or using ICT-based information and ICT resources owned/managed, supported or operated by, or on behalf of the KFC.

(a) All users should be aware that several network usage issues are covered by the National ICT Policy, violation of which is an offence under national law. (b).The College LAN and Internet access resources are meant for official use arising from the academic/research activities and administrative responsibilities of the staff and trainees of the college. (c).Users should view the ICT & network resources with a sense of ownership and participation, and should actively help to prevent any misuse. Procedures laid down from time to time regarding the management of ICT & network resources, must be understood and followed meticulously by the user community. (d). The ICT Support Unit has the right to monitor and scan all information carried by the network for the purpose of detecting and identifying inappropriate use. As such the privacy of information carried by the network is not guaranteed. ICT Support Unit is authorized to break open a PC **or** disconnect it from the network, if called for. However, specific scanning will be done only on approval by the managment upon detection of policy breach. This is in accordance with the National ICT Policy.

5. PRINCIPLES:

This policy shall be guided by the following key principles

a. Mainstreaming of ICT in the College.

b. Seamless integration of ICT with other College activities/programmes.

c. Inclusion, flexibility and support of other quality Management Systems.

d. Adherence to best ICT Practices and Policies in currently in use.

6. SCOPE:

The ICT policy document covers all KFC offices, facilities and ICT resources including, but not limited to installed ICT systems *i.e*. ERPs, email, Internet, databases, operating systems (windows, Linux/Unix), Internet protocol telephone systems, wireless communication, printers and copiers.

7. APPROVAL OF POLICY DOCUMENT:

This document becomes effective from the date of approval by the Board of Directors for Kenya Forest Service.

8. CRITICAL INFORMATION SECURITY

Definition:
Critical Information Classification is the classification of information based on its level of sensitivity and the impact to the College should that information be disclosed, altered or destroyed without authorization. The classification of information helps determine what basic security controls are appropriate for safeguarding that information. All College information should be classified into one of three sensitivity levels, or classifications:

Restricted Information, which is highly valuable and sensitive. The unauthorized alteration, disclosure or loss of this information can cause significant damage (devastating) to the College, for example, examination results under process, accounts, status of security etc. This information must be highly protected as it cannot be easily recovered or brought to its original state easily.

Private Information, which is of moderate importance and sensitivity. Its unauthorized alteration, disclosure or loss of this information can cause moderate damage to the Institute. Generally, the information which is not classified in other two classes falls under this. Reasonable and effective security is required for this information, as recovery of its original state may take sizable amount of resources.

Public Information, which is of low importance and sensitivity. Its unauthorized alteration, disclosure or loss of this information can cause little damage to the College.

Public information includes press releases, circulars, notifications, course information and research publications, published results on website etc. While little or no controls are required to protect the confidentiality of Public information, some level of control is required to prevent unauthorized modification or destruction of Public information.

All information created, processed, generated, maintained and deleted by the College must be classified into these categories and different levels of user privileges must be defined for each function. Only authorized users can get access to the category of information he/she is authorized to access.

9. NETWORK DEVELOPMENT AND MANAGEMENT:

The network infrastructure at KFC is composed of a LAN and WAN. This integrates voice, data and video, to form a unified information technology resource for the College. The network therefore demands adherence to a centralized, coordinated strategy for planning, implementation, operation and support. The policy defines the arrangements and responsibilities for the development, installation, maintenance, use and monitoring of the ICT networks to ensure that, they are adequate, reliable and resilient to support continuous high levels of activity.

9.1 INSTALLATIONS OF ICT NETWORKS:

a. Installation, configuration, maintenance, and operation of all networks including wireless networks serving on any property owned by the by the College through Service, are the sole responsibility of ICT Section.

b. All requests for installation of network device or active networks for instance routers, switches and wireless access points must be approved by Head, ICT Section at the College.

9.2 CONNECTING TO THE ICT NETWORK:

All connections to ICT networks shall be governed by the following principles:

a. Before access is granted to ICT resources, users will be required to read the ICT Security AND Usage document and sign the User Acceptance Form (Appendix 1)

b. All computing devices that are connected to ICT network should be properly protected against hacking, viruses and similar security threats, through appropriate use of security technology.

c. Users of portable computer and data communications devices who wish to directly connect to the network will require authorization from Head, ICT.
d. The Service reserves the right to limit access to its networks.
e. Personal computers which store data that violates ICT policies can be disconnected from the network without notice.

9.3 EXTERNAL ACCESS TO SERVERS ON THE ICT NETWORK:

External access means access to the College's ICT network by approved service providers from external locations.

a. Where specific external access is required to servers on the ICT network, the ICT section shall ensure that this access is strictly controlled and limited to specific external locations or persons.
b. The ICT Section will monitor compliance with access arrangements.
c. Misuse or failure to comply with these arrangements shall result in immediate restriction or disconnection from the network.

9.4 NETWORK SECURITY:

a. ICT shall install Firewalls and Intrusion Detection systems across the entire KFC network to monitor and prevent hackers, viruses and worms including all other forms of attack.
b. All computers hooked into the network shall mandatorily have up-to-date antivirus software to prevent viruses and all other forms of malicious.
c. All servers shall likewise have antivirus and a form of monitoring to ensure that only authorized users have access.
d. All staff and trainees are also expected to seek authority from ICT section before hooking any private laptop/desktop/mobile device (Ipads/Tablet, Smartphone *etc.*) to the KFS/KFC network.
e. Access to wireless networks should be password protected i.e. before login to wireless networks; one is required to use a password. ICT shall ensure this is enforced.

f. It shall be the responsibility of ICT section to ensure that this is adhered to failure to which may result to disciplinary action.

9.5 SUSPENSION AND TERMINATION OF ACCESS TO ICT NETWORKS:

A user's access to the College ICT networks shall be revoked automatically:

a. Upon exit from the Service/College.
b. At the request of the Principal.
c. On suspension pursuant to a disciplinary proceeding.
d. The College management shall put in place mechanisms to ensure that changes in staff employment status are communicated to ICT Section appropriately in order to revoke access to ICT Network.

10. ICT SYSTEMS AND EQUIPMENT USAGE:

The Service/KFC provides ICT computing resources to its staff and trainees for official use as part of enhancing business operations; The College will encourage an ICT use culture to improve efficiency. Access to the Service's ICT resources comes with responsibilities of proper use.

The following guidelines in relation to ICT systems and equipment usage shall apply;

a. Only authorized users are allowed to access the College ICT Systems. Authorized users are prohibited from sharing computer accounts, passwords, and other types of authorization assigned to them. Such users are exclusively responsible for use of their accounts.
b. The authorized users shall utilize the ICT resources ethically and responsibly. Any user using the Service's ICT resources to for example harass, violate privacy, waste resources or interfere with data integrity, violation of software license or other copyright agreements shall be subject to existing Service regulations and procedures.
c. Authorized users must strictly observe equipment operation instructions including messages generated by the various systems for example PCs, printers, photocopiers and scanners. In cases of doubt technical assistance should be sought from ICT support desk.

d. Authorized users shall not run or otherwise configure software or hardware to intentionally allow access by unauthorized users. Deliberate attempts to degrade the performance of a computer system or network or to deprive authorized staff of resources or access to any computer or network is prohibited**.** Users are also prohibited from using any computer program or device to intercept or decode passwords or similar access control information.

e. When an authorized user changes status (e.g.; terminates employment, retires, changes positions or responsibilities within the College or completes training or is expelled from the training), the HR Division or Department responsible for initiating that change in status must coordinate and inform ICT section to ensure that access authorization to all organization resources is appropriate. An individual shall not use facilities, accounts, access codes, privileges, or information which is not authorized.

f. At the point of departure from the Service/college all staff/trainees will be expected to surrender the computing equipment (desktop, Laptops, and Printers) issued to them. The equipment should be deposited with the stores after confirmation by ICT Section on the condition. The staff/student/s will be held responsible for any loss.

g. No software may be installed, copied, or used on the Service's computing resources except as permitted by the Service and the legal owner of the software. Software subject to licensing must be properly licensed and all license provisions (installation, use, copying, and number of simultaneous users and term of license.) must be strictly adhered to. ICT Section is the custodian of all software and licenses in the Service.

h. Only ICT staff are authorized to install approved and licensed software in the Service's ICT equipment.

i. Users are prohibited from installing software in their desktops/laptops without ICT authority/approval. The Head of ICT Section shall ensure that computer accounts are **not** set as administrators, but as users only.

11. SOFTWARE DEVELOPMENT AND SUPPORT:

a. To ensure information systems reliability, all in-house and outsourced system developments shall be planned for, incorporated in the process of software development which follows the due process right from the planning phase through to the implementation stage and that all deliverables at every milestone meet the required standards.

b. Once software has been adopted and is operational, there is need to ensure that all necessary support and use procedures are adhered to.
c. ICT Section shall be responsible for development and maintenance of ICT systems.

11.1 OUTSOURCED SYSTEMS:

a. Divisions/Departments may be allowed to buy software or customize software limited to internal usage after consultation with Head, ICT.
b. ICT Section shall verify if proposed software is compatible and conforms to standard software/operating system development.

11.2 IN-HOUSE SYSTEMS:

ICT Section will assist in development, maintenance and support of systems that best suits the Colleges' needs. In developments of such systems, prior requests and approvals are made to Head of ICT Section.

11.3 SYSTEM SUPPORT:

ICT Officer shall ensure that every system implemented shall be provided with essential support service to guarantee continuity of services.

12. ICT EQUIPMENT REPAIR AND MAINTENANCE:

a. ICT Section shall maintain all equipment required by users for use in their offices to perform day to day duties.
b. ICT Section shall **not** be responsible for maintenance of personal equipment.
c. ICT Section shall prepare a schedule of preventive maintenance as per the manufacturer specification.
d. All ICT equipment repairs shall be the sole responsibility of ICT Section.

12.1 ICT EQUIPMENT REPLACEMENT:

a. The life cycle of the hardware varies depending on the equipment type. On average, ICT hardware may be replaced at least after every five (5) years in accordance with user needs and change in technology. While for software the life cycle is dependent on the release of the new versions in accordance with the software maintenance agreement.
b. ICT equipment determined to be still useful and still meets the required safety standards may be reassigned to lesser demanding tasks or appropriate environment.
c. ICT hardware shall be declared obsolete according to the need of the Service and the recommendations of maintenance team.
d. The disposal of obsolete equipment shall be governed by the Public Procurement and Asset Disposal Act 2015.
e. ICT Section shall ensure data hard drives are completely formatted before disposal.

12.1.1 REPLACEMENT OF LOST ICT EQUIPMENT:

a. The holder/user **must** implement and observe adequate physical safety procedures against theft.
b. Loss of ICT equipment should be **immediately** reported to **Principal** for appropriate action.
c. The report to the Principal **must** be supported by the following documents;
    i. Police abstract
    ii. Detailed report of how the loss happened
d. It is only upon satisfactory report that a user's ICT equipment is replaced, otherwise the user is surcharged.
e. Head of ICT Section upon receipt of the loss report forwards through the Principal to Legal Department to initiate insurance replacement.

13. ICT PROCUREMENT:

Hardware Asset Identification

A team of staff consisting from the User Department, procurement and ICT section will identify the appropriate hardware required to provide ICT services at the College. The procurement process will be guided by the following;

a. Procurement of ICT related goods and services shall be done in accordance to the applicable procurement laws.

b. All ICT related procurements will only be undertaken after the following;

   i. The intended procurement is included in the procurement plan for the requesting division or department.

   ii. This procurement is captured in the ICT Section consolidated procurement plan and budget is available.

   iii. The request is fully approved by the Principal.

   iv. For users with existing ICT equipment, either the old equipment has reached end of life, current duties require a more powerful equipment or any other approved justification for new procurement.

c. After approval, ICT Section shall provide the following services:

   i. Prepare technical specifications in consultation with Head, ICT at KFS

   ii. Evaluate procured goods and services.

   iii. Inspect delivered goods and services to ensure they meet specifications.

ICT Section shall ensure that hardware is properly insured after procurement. This will ensure that in the event of theft or accidental damage, the same is taken care by the insurance.

14. INVENTORY OF ICT EQUIPMENT AND SOFTWARE:

a. The ICT Section shall be responsible for keeping an up -to-date inventory of the hardware and software that is in use at the Service's offices.

b. Head of ICT shall keep an inventory of approved/licensed software.

c. Movement of ICT equipment within or out of KFC must be authorized by ICT officer and the Principal.

14.1TRANSFER/MOVEMENT OF ICT EQUIPMENT:

a. All ICT equipment that requires movement outside the office must have a gate pass approved by Head, ICT Section and the Principal.

b. Security at the gate are required to check whether movement is duly approved by ICT Section and Principal with the details well documented such as;

    i. Equipment type e.g. laptop, desktop etc.

    ii. Serial number

    iii. Reason for movement

c. For change of ownership, ICT Section **must** be notified in order to update its inventory.

15. PRINTING AND PHOTOCOPYING OF DOCUMENTS:

Printers and photocopiers shall be centrally located to ease sharing. Use of soft copies is encouraged to minimize on printing costs. Individual printers are discouraged.

16. SOFTWARE LICENSING:

a. The College shall ensure that only licensed software is installed in ICT equipment in compliance with software licensing laws. It will also ensure that this license is renewed when due.

b. Alternative software e.g. open source will be evaluated from time to time so as to assist the College in cutting costs. The evaluated software will require approval from ICT officer in liaison with Head, ICT Section before being installed on production systems.

17. INTERNET USE:

Internet is a key tool of work in all organizations. The College allows all staff and trainees to access the internet for business purposes. The College will monitor internet usage and block inappropriate sites.

Social media sites are only open to users whose duties require use of these sites during working hours.

18.0 APPLICABLE POLICIES:

A number of policies have here below been provided to ensure the effective and efficient implementation of ICT usage at the College.

18.1 ANTI-VIRUS AND ANTI-SPAMMING:

The purpose of the College's antivirus and anti-spamming policy is to ensure the College has adequate protection from computer viruses, unwanted and unsolicited mails both internally and externally by deploying an antivirus and anti-spamming software on College owned facilities.
The College provides licensed antivirus software that is deployed to college owned facilities.
All users within the College are to ensure their personal computers have up-to-date and licensed antivirus software running on their machines.

The ICT Section will:

a. Employ virus management measures at appropriate points of the College network.
b. Implement virus control software and procedures to ensure that all networked computer servers and ICT managed workstations are protected against virus infection.
c. Immediately disconnect compromised ICT facilities and services from the College network and these will remain disconnected until the infection has been remedied.
d. Disconnect from the College network any user-owned or leased equipment that does not have appropriate and maintained antivirus software installed.
e. Monitor continuous update of the anti-virus software installed.

18.2 BANDWIDTH USAGE:

KFC is dedicated to ensuring efficient and fair network utilization with the intention to meet the growing bandwidth requirements of the entire college.
The purpose of the guideline is to ensure that the KFC community has a clear understanding of proper procedure and usage, and to ensure that all users are able to obtain their fair share of the wired/wireless network.

This guideline applies to all KFC affiliates that are; trainees, faculty and other staff members as well as guests.

Management of bandwidth resources shall be entrusted to the ICT Section.

The following will apply;

a. Internet bandwidth will not be over utilized as to prevent access to critical information, research and online educational materials.
b. Unauthorized persons/users are not allowed to access internet facilities within the campus network.
c. ICT resources shall be monitored at all times by the ICT Section for efficiency and optimal usage by all the users.
d. Use of internet is allowed as long as it does not violate the policy or degrade the performance of the network or divert attention from work or studies.
e. No user may damage, alter, or degrade equipment providing internet and network connections, thus hindering others in their use of the Internet.
f. In cases where a user has been asked to disable a service, and does not do so, the ICT Section may revoke access to the network and initiate appropriate disciplinary procedures against the user. Disciplinary actions may include loss of network access for 30 days or more.

Users shall not:

a. Download or store music, media or any other files where copyright issues may be of concern.
b. Use the College Internet facility for running private businesses.
c. Upload, download, or transmit.
d. Copyrighted materials belonging to third parties.
e. Offensive, fraudulent, threatening or harassing materials.
f. Propagate computer viruses, run peer-to-peer software, send and/or receive unofficial files or undertake activities that cause network congestion.
g. Use KFC facilities to gain unauthorized access to any computing, information, or communications devices or resources.

18.3 SYSTEM BACKUPS:

The College shall formulate and implement systematic procedures for performing backups on the implemented systems.
Detailed backup steps are indicated in the backup procedures.

18.3.1 BACKUP OF USER AND INDIVIDUAL DATA:

a. For individual user workstations and laptops with critical organization data, users shall use portable external disks to backup individual data.
b. Critical college data shall be backed up on shared network folders under guidance from ICT section.
c. ICT section MUST ensure that the holder/user of the Laptop/mobile computer recognises their responsibilities in this regard.

18.3.2 ADDITIONAL ICT SECURITY GUIDELINES

Additional ICT security guidelines are detailed in KFS and KFC ICT security & usage documents.

18.4 E-MAIL USAGE:

E-mail is formally recognized as a form of official communication and is provided to all staff in the College.

Corporate E-mail shall be used for official correspondences. Staff members shall not use E-mail services for the following:

a. Sending offensive, intimidating, harassing or humiliating emails to staff or other persons.
b. Transmitting material that includes false claims of any deceptive nature.
c. Sending forged messages, obtain or use someone else's e-mail address and password without their authorization.
d. Attempting to gain access to e-mail messages addressed to any other employee without first obtaining authority from the addressee or an appropriate level of management

e. Sending chain letters, or advertising material which does not relate to KFC/KFS’s business
f. Sending, distributing, storing or printing e-mail of a sexually explicit, racist or offensive nature, or invite or encourage others to do so. If any material of the such kind is received, it should be reported immediately to the ICT support department and if the email is received from an internal source then the sender should also be contacted to make them aware in case they have unknowingly contracted a virus.
g. Inappropriate use of e-mail may lead to disciplinary measures in accordance with applicable Service regulations

18.5 ICT SECURITY:

The college shall ensure security of all ICT resources and information systems. This shall be achieved by ensuring development of security measures and procedures in the following areas;

a. Physical infrastructure
b. Information and data

18.5.1 ACCESS TO NETWORK CABINETS:

a. All network cabinets shall be under lock and key at all times.
b. All cabinets should be connected to UPS and surge protectors to protect the equipment in the event of power surges

18.5.2 PASSWORDS USAGE:

a. Passwords are the entry point to all ICT resources. Protecting access to resources is pivotal in ensuring that systems remain secure.

The College shall develop and regularly update procedures on password use to protect ICT resources.

19. USER SUPPORT AND MAINTENANCE:

ICT systems play a major role in supporting the day to day activities of the College. Maintenance and Support of the ICT systems is essential to the success of academic and administrative activities.

Purpose:

The purpose of this policy is;

a. To provide a framework for the best operational practice, between the ICT Section and the users; that enables all involved to save time and provide any ICT assistance that may be required.

b. To ensure that all the College's ICT systems, programs, data, network and equipment are functional.

c. To ensure that all the users are responsible for reporting immediately any malfunctions of any ICT equipment to the ICT Section.

User support is open to all computer hardware and software owned by KFC and all users of computer systems, including but not limited to college faculty, trainees, and staff.

The areas of support include equipment repair and preventive maintenance.

19.1 COMPUTER LABAROTORY USAGE:

KFC has set up computer labs for academic, instructional, research, administrative and public service purposes. Computer labs are to be kept functioning at an optimal level of effectiveness for all users.

All persons using KFC computer labs and equipment must abide by this policy.

The following shall apply;

a. Persons using Computer laboratory equipment must have a KFS/KFC ID card valid for the current semester and must be able to produce the card upon request.

b. All persons using the lab are responsible for backing up their own data and protecting their own information.

c. Smoking, food and beverages, are prohibited in the labs.

d. Audio output or sound playing devices are permitted only with the use of headphones.

e. KFC lab equipment may not be used for business purposes or in any for-profit venture.

f. Disabling computers by disconnecting cables, removing hardware, installing software or locking workstations will be considered vandalism and treated as such.

The following procedure will be following;

a. The computer lab is open during the semester and office hours.
b. The computers in the computer lab all have an updated antivirus. Therefore, trainees can freely use their removable storage media.
c. All problems or assistance should be reported to ICT Section.

19.2 WEBSITE USE AND MAINTENANCE:

The College shall maintain an up to date College website for communicating with its various stakeholders. The following shall apply to website content uploads;

a. All website upload requests shall only be acted on after users have completed an upload approval form which is dully filled and approved as appropriate.

b. The website content shall be updated and reviewed on regular basis.

Purpose:

The Kenya Forestry College website/page is designed to make it easier and more efficient for visitors to learn about and interact with Kenya Forestry College.

Like all online resources, we recognize that website visitors are concerned about issues of privacy, security of information, the quality and accuracy of the information presented. The mission of the KFC website is to:

a. Provide a means of communicating news and information regarding KFC to the general public, academic communities elsewhere, faculty, trainees, and staff within the College.
b. Act as a resource for research and education for the general public, academic communities, faculty, trainees, and KFC staff.
c. Highlight and showcase the exciting and original ongoing research and innovation at the college, as well as the academic and educational accomplishments of the College.

KFC is committed to preserving privacy and security while visiting the website and to giving the best possible information. KFC may, at its sole discretion, change, modify, add or delete portions of this policy.

This Policy also applies to all KFC administrative officers and Heads of Departments who are in charge of providing information for respective website/webpage(s).

Copyright:

All materials posted on the site are subject to copyrights owned by the KFS/College or other individuals or entities. Any reproduction, retransmission or republication of all or part of any posting or document found on the site is strictly prohibited, unless KFC or the copyright owner of the material has expressly granted its prior written consent to so reproduce, retransmit or republish the material. All other rights are reserved.

Responsibilities:

The day-to-day operation of the website will be overseen and maintained by the ICT Section.

The College Principal can either allow updates to be live, if compliance is confirmed or contact the author for amendments.

Procedure to Ensure Website is up to Date:

The College website will be updated regularly.

Any person requesting a webpage update, revision or inclusion must submit a written request to the relevant Head of Department for approval before communicating to the ICT Section.

Upon submission, all requests will be reviewed and the person will be contacted via e-mail or phone regarding the status of the request. Any updates to a web page must be submitted in their entirety before an update begins. For instance, if one of your web pages needs to be updated, you must submit all text and images required to update that page.

Limit of Liability:

KFC may not be held responsible for any loss or damage arising from use of the College website/page.

The ICT Section may not be held responsible for any mistaken or outdated content on the KFC website/page.

19.3 HARDWARE AND SOFTWARE DISPOSAL /ICT ASSET DISPOSAL AND E-WASTE MANAGEMENT:

The term e-waste is a generic and encompasses various forms of electronic and or electrical goods that are old have reached shelf life or have ceased to be of any value to the owners (UNEP Definition).

Kenya Forestry College shall and dispose of all technology hardware and software in environmentally friendly manner and in the relevant accordance to disposal laws and the Kenyan laws, including, but not limited to regulating waste and respecting copyright and licensed software. We aim as much as possible to avoid creating e-waste.

In the event that College technology hardware or software is no longer required due to:

a. Excess of useful life
b. Lack of continued need
c. Inability to upgrade required hardware or software
d. Damage
e. Excessive maintenance cost
f. Reception of a new computer

The corporate disposal of assets shall apply and;

a. All such equipment must be evaluated by both the ICT Section and the Head of relevant Department in accordance to the Policy.
b. Disposal is through the Procurement Department of the College.

Based on the assessment of the equipment the following process will be followed:

-Redistributed

If a computer meets current minimum standard requirements, it will be redistributed to a location within the college based on the overall needs of the college.

-Donated/ Sold

Any hardware considered no longer in service to the College can be donated/sold to:

a. Non-profit educational institutions.
b. Non-profit organizations.
c. Any interested person/company.

The ICT Section will ensure the hardware is cleared of all software licensed to the College and any data.

-Salvaged

Any hardware that can no longer be used, but which has useful parts, will be salvaged for its parts. Those parts could be used by the ICT Section.

-Disposed off

Computer hardware and peripherals, which cannot meet the above categories, will be disposed. This equipment will be picked up by a reputable environmentally certified recycling company in compliance with all state laws.

Any equipment, which is donated, salvaged, or disposed, will have a completed disposal record form.

Request for approval for disposal will be provided by the Head of ICT and endorsed by the Principal.

19.4 ICT TRAINING:

The College recognizes the need for ICT training and development of all its users to achieve its mandate. Training shall focus on building skills in users to make them effective in exploiting provided ICT resources.

To ensure that users have sufficient knowledge of operating computer systems, current technology and job demands: -

a. Internal ICT user training targeting users shall be scheduled on a continuous basis.
b. External ICT training shall be organized by the ICT Department in response to needs as may be assessed from time to time when training is not possible within ICT.
c. The Service shall facilitate training of ICT staff consistently to act as the first level ICT Support on all installed ICT systems.
d. For newly acquired ICT systems, it is a requirement that technical training is included in the scope of works and must be provided by the supplier or consultant during implementation. This will ensure that ICT technical staffs are able to use, manage and train other users on the new systems.

e. ICT training needs assessment shall be conducted on regular basis.

19.5 E-LEARNING:

E-learning policy is designed to support college e-learning activities. This will enable KFC carry out its online activities by protecting and preserving College ICT resources at the appropriate level.

The College intends to facilitate access to and coverage of education by using ICT in instruction, learning and research through the approved E-learning platforms.

The College will:

a. Create organizational (trainer capacity, training management) and technical (practice lab and computer-based training tools, self-paced training modules conditions assuring continuous in-house e-learning training capabilities in the long-term.
b. Ensure and require that all trainees and academic staff are trained on a continuing basis to equip them with the requisite skills to fully exploit the digital learning environment in their different disciplines.
c. Develop university-wide and contribute to global e-learning networks based on academic interests groups and research collaborations.
d. Establish the appropriate infrastructure and software responsive to academic needs through the designated central technological unit.

The E-Learning Goals will include;

a. To provide an electronic education delivery system for greater access by our trainees;
b. To provide flexibility of time and location;
c. To promote the integration of technology in the learning environment
d. To promote globalization of education through electronic access to information and experts worldwide.
e. To identify, provide, expand, and coordinate the development of quality courses and programs to meet the needs of e-learners.

f. To Encourage and support the use of the learning and other technologies in both face-to-face and online learning environments.
g. To evaluate periodically and comprehensively every facet of the e-learning program and use these results to restructure and improve the program.
h. To ensure and require that all trainees and academic staff are trained on a continuing basis to equip them with skills to fully exploit the Digital Learning Environment (DLE) in their different disciplines.
i. To establish the appropriate common DLE infrastructure and software responsive to academic needs through the designated central technological unit.
j. Units shall develop and nurture complementary methods of teaching and learning to e-learning as a medium of distance learning both within campus and outreach /upcountry centers, in the long term.

Trainee's Privacy:

All trainees will have an e-learning account created when they join KFC. They will be enrolled in the courses they are pursuing for the semester/term and will have access to the courses.

Trainees will only have access to their particular account and be advised to set up a strong password.

The Lecturers will grade the assignments that they give and the marks will only be visible to the particular trainee, thus ensuring trainee's privacy.

E-Learning Training/Support:

The ICT Section will train new trainees on how to login, access and download class notes as well as upload class assignments as given by the lecturers.

The ICT Section will also train new faculty on how to login, access, upload class notes and class assignments. They will also be taken through the process of downloading and grading assignments.

The ICT Section will offer support to every user of the LMS experiencing difficulties troubles.

The person experiencing difficulties will be expected to write an email or make a phone call to bring to the attention of the ICT Section that they have troubles. The trouble shooting will be resolved at the earliest time possible.

Virtual Classroom:

A virtual classroom is an online classroom that allows participants to communicate with one another, view presentations or videos, interact with other participants, and engage with resources in work groups. The virtual classroom will run on Zoom software by Zoom Video Communication. This is free software that allows one to make a video call for 60 minutes. In order to use the classroom, the faculty and trainees will be required to make a reservation to avoid double booking. Responsible use of equipment in the room is highly encouraged in order to serve the users well.

Only those who have undergone the Virtual Classroom training will be allowed to use the room. Faculty will also make use of the Google classroom platform to conduct instruction.

20. ICT IMPLEMENTATION GUIDELINE:

The implementation of this policy shall be the responsibility of management of KFC. The Head of ICT section shall monitor the implementation of this policy.

The ICT policy implementation exercise is dependent on obtaining approval and support from the College management. The commitment of the Management will enable establish a cohesive link between the College's objectives and the ICT Policy.

It is the responsibility of the ICT Section to inform Management in advance of the financial year of every support required of the KFC management.

The College management will fulfill the following responsibilities:-

Strengthening of the ICT Section - KFC shall strengthen the ICT Section as the department in charge of daily operation of ICT and the lead in the implementation of the ICT Policy.

Recruiting and retaining qualified personnel - Because of the complex, constantly evolving nature of the ICT industry, it is of critical importance that the College employs and retains qualified staff to enable a successful implementation of the ICT policy.

Violations of this policy shall be addressed by appropriate KFS/KFC mechanisms.

21. NOTIFICATION:

The College management shall inform all persons subject to this Policy of its terms as soon as efficiently possible after its adoption and at regular intervals thereafter. Every effort will be made to aggressively publicize the policy and make it widely understood and accepted, by holding training sessions for end users, circulating training material, organizing personal meetings and posting notices to that effect.

22. MONITORING AND IMPLEMENTATION:

a. The implementation of this policy shall be the responsibility of management of KFS.

b. Head, ICT shall monitor the implementation of this policy

c. Violations of this policy shall be addressed by appropriate KFS/KFC mechanisms.

Statement of Policy:

All users of the ICT facilities of KFC will be subject to the following Acceptable Use Policy and bide themselves to;

(a) Be responsible for all use of this network. In case I own a computer and decide to connect it to KFC network, I will be responsible for all the content on it, especially that which I make available to other users. (This provision will also apply to any computer or device for which I am responsible, and is included in the meaning of “my computer”.) In case I do not own a computer but am provided some ICT resources by KFC, I will also be held responsible for the content stored in the designated workspace allotted to me (examples: file storage area, web pages, stored/archived emails, on ICT Support Unit or Department machines).

(b) Be held responsible for all the network traffic generated by “my computer” understanding that network capacity is a limited, and shared resource. I agree that physically tampering with network connections/equipment, sending disruptive signals, or making **excessive use** of network resources is strictly prohibited. Repeated offenses of this type could result in permanent disconnection of network services. I shall not share the network connection beyond my own use and will not act as a forwarder/ masquerader for anyone else.

(c) Understand that the ICT infrastructure at KFC is for official use and shall not use it for any commercial purpose or to host data/network services for other people or groups. Also, I shall not host or broadcast information that might harm others or may be otherwise considered objectionable or illegal as per provisions of Kenyan law.

(d) Not attempt to deceive others about their identity in electronic communications or network traffic. I will also not use KFC ICT resources to threaten, intimidate, or harass others.

(e) Not intrude on privacy of anyone. In particular I will not try to access computers (hacking), accounts, files, or information belonging to others without their knowledge and explicit consent.

(f) Understand that the ICT resources provided to me are subject to monitoring, with cause, as determined through consultation with the KFC administration, when applicable. The monitoring may include aggregate bandwidth usage to effectively manage limited ICT resources as well as monitoring traffic content in response to a legal or law enforcement request to do so. I authorize KFC management to perform network vulnerability and port scans on my systems, as needed, for protecting the overall integrity and efficiency of College network.

(g) I shall maintain my computer on this network with current Antivirus/Internet Security/Endpoint Protection software and current updates of my operating system, and I shall attempt to keep my computer from viruses, worms, Trojans, bots, malware and other similar programs.

(h) Not to use the ICT infrastructure to engage in any form of illegal file/data sharing (examples: copyrighted material, obscene material).

(i) Understand that I will not take any steps that endanger the physical or logical security of the KFS network. Specifically, I will not attempt to bypass firewalls and access rules in place. This includes not setting up servers/communication devices (including wireless) of any kind (examples: web, mail, proxy, router, managed or unmanaged switch, smart phones) that are visible to the world outside the KFC campus. In critical situations, KFC management reserves the right to disconnect any device or disable any account if it believed that either is involved in compromising the information security of KFC.

(j) Understand that any use of ICT infrastructure at KFC that constitutes a violation of KFC Regulations or provisions of Kenyan Cyber Law could result in administrative or disciplinary or legal procedures. Your access will be automatically **suspended/blocked** completely, if the ICT Infrastructure Access Policy is not **accepted** or **abided** by you.

23. BUSINESS CONTINUITY MANAGEMENT:

The College through the service shall have a Business Continuity Plan (BCP) that will be implemented for all critical ICT systems. The BCP shall be documented and marinated to ensure that where disasters may occur normal services remain always available.

Change Management Policy:

This change management policy is aimed at ensuring College business continuity.

Definition:

Change Management is purposeful control of any change which may affect financial reporting, operations or compliance. This includes the Control Environment (i.e. all systems business processes including IT which may impact on the above).

Policy Statement:

The Change Management Policy shall help to communicate the Management's intent that changes to ICT supported business processes will be managed and implemented in a way that shall minimize risk and impact to KFC's operations. All intended changes to IT systems shall be required to follow an established Change Management Process. IT systems will be subject to a formal change management process that ensures or provides for a managed and orderly method by which such changes are requested, approved, communicated prior to implementation (if possible), and logged and tested.

Purpose:

The purpose of this policy is to establish management direction and high-level objectives for change management and control. This policy will ensure the implementation of change management and control strategies to mitigate associated risks such as:

(a). Information being corrupted and/or destroyed; (b).Computer performance being disrupted and/or degraded; (c).Productivity losses being incurred; and (d).Exposure to reputation risk.

Scope:

(a) Employees/Trainees

This policy applies to all parties operating within the organization’s network environment or utilizing Information Resources. No employee/trainee is exempted from this policy.

(b) IT Assets

This policy covers the data networks, local servers and personal computers (stand-alone or network-enabled), located at offices and depots, where these systems are under the jurisdiction and/or ownership of the organization, and any personal computers, laptops, mobile devices, and servers authorized to access the organization’s data networks.

Policy documentation shall consist of Change Management Policy and related procedures and guidelines.

Document Control:

The Change Management Policy document and all other referenced documents shall be controlled. Version control shall be used to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

Records:

Records being generated as part of the Change Management Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

Distribution and Maintenance:

The Change Management Policy document shall be made available to all the employees/trainees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the document shall be with the ICT support and system administrators.

Privacy:

The Change Management Policy document shall be considered as “confidential” and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

24. REVISIONS:

a. This policy shall be reviewed after a period of three (3) years.

b. The changes necessitating review shall include change in technology, evolving global trends, statutory regulation (legislation) and any other reasons as may be determined from time to time by the Head, ICT.

25. DOCUMENT CONTROL:

Document Name:	ICT Policy
Prepared by:	Principal, KFC/ Head, ICT
Revision	0
Reviewed by:	KFS Senior Management
Approved by:	KFS Board of Directors
Signature by CCF	
Date Approved:	
Effective Date:	23rd September, 2020

ICT SECURITY AND USAGE POLICY

This approved ICT Authority document has been customized for KFC usage.