INFORMATION & COMMUNICATION TECHNOLOGY POLICY 2019

FOREWORD

The Forestry Commission (FC) ICT Policy Document 2019 demonstrates the progress made by the Forestry Commision in the use of Information & Communications Technology (ICT) infrastructure and resources for doing business efficiently and effectively.

The FC has found it very necessary to formulate this policy to ensure optimum benefits of the use of IT resources to manage the potential risk of ICT. It is also to prevent the abuse of ICT resources, optimize cost, and ensure that its Employees and users are aware of their responsibilities and the potential consequences of a breach and the liabilities imposed on them.

It has become increasingly evident given its importance as a strategic asset, that the employees of FC must adhere to strict compliance with stated guidelines concerning the appropriate use of its ICT resources. These include hardware and software systems, networks and other facilities administered by the Corporate Headquarters, as well as those administered by Divisions, Departments and Units.

The use of ICT resources, even when carried out on a privately owned computer is governed by this Policy.

This Policy Document also provides the principles to which all users must adhere to, when handling information owned by or entrusted to the FC in any form. This ICT Policy Document, is also well-anchored within the national ICT policy and legal environment.

It is my hope that users of this ICT Policy Document, will gain a better understanding of how ICT resources will have to be used and deployed as a means of enhancing productivity, efficiency and effectiveness in the delivery of our mandate.

This Policy will be reviewed biennially to respond to the fast changing ICT environment and ensure that the FC derives maximum benefits from its ICT investments.

In conclusion, I wish to reiterate FC's commitment to ensure strict compliance with this Policy without fear or favor to enhance productivity, efficiency and effectiveness in the delivery of our mandate.
Thank you.

KWADWO OWUSU AFRIYIE
Chief Executive

TABLE OF CONTENTS

LIST OF ACRONYMS

ACRONYM	MEANING
DRS	Disaster Recovery Site
FC	Forestry Commission
FCHQ	Forestry Commission Headquarters
FCTC	Forestry Commission Training Centre
FSD	Forest Services Division
GPS	Global Positioning System
ICSA	International Computer Security Association
ICT	Information and Communication Technology
ISP	Internet Service Provider
LAN	Local Area Network
LCD	Liquid Crystal Display
PDA	Personal Digital Assistant;
RMSC	Resource Management Support Centre
TIDD	Timber Industry Development Division
TNA	Training Needs Assessment
UPS	Uninterruptible Power Supply
VPN	Virtual Private Network
WAN	Wide Area Network
WD	Wildlife Division

SECTION ONE

1.1. INTRODUCTION

The introduction of corporate-wide use of Information & Communications Technology (ICT) infrastructure has brought about a common platform for doing business effectively and efficiently. The increased efficiencies created from the use of Local Area Network (LAN), Virtual Local Area Network (VLAN), Wireless Local Area Network (WLAN), Wide Area Network (WAN), Intranet, Internet and Virtual Private Network (VPN) have also introduced new risks. The FC has therefore found it very necessary to formulate this policy to manage the potential risk of ICT, prevent the abuse of ICT resources, optimize cost, and ensure that Users are aware of their responsibilities and the potential consequences of a breach of these responsibilities to the Forestry Commission (FC) and the liability imposed on them.

Violations of this policy will be handled in accordance with the Terms and Conditions of the Forestry Commission under which offences are classified as Minor, Major and Intolerable and specifically in reference to ICT, the classification is as provided in Annex 3.

1.2. PURPOSE

Users of ICT resources of FC must adhere to strict guidelines concerning the appropriate use of these resources. This policy provides guidelines for the appropriate use of the Commission's ICT resources. It also provides the principles to which all users must adhere to when handling information owned by or entrusted to the Commission in any form.

1.3. SCOPE

The terms and conditions described in this policy apply to all Users of data and all computer systems. These include hardware and software systems, networks, and facilities administered by the Corporate Headquarters, as well as those administered by individual Divisions, Departments and Units. The use of ICT Systems, even when carried out on a privately owned computer that is not managed or maintained by the Commission, is governed by this Policy. This document also addresses the Commission's ICT policy with regard to:

i. The correct and proper use of the Commission's data and computer systems

ii. Users' access to the internet provided by FC
iii. E-mail sent and received by Users via among others, the Commission's Corporate Email System.

1.4. POLICY OBJECTIVES

The objectives of the policy are to:

i. Ensure the integrity, reliability, availability and good performance of ICT resources.
ii. Ensure that ICT resources are used for their intended purposes within FC.
iii. Encourage ethical and lawful behaviour by users and providers of information.
iv. Detail the consequences of inappropriate use of Commission's data and/or resources.
v. Provide a guideline for protecting the Commission's data and/or information resources from theft, loss, damage and unauthorized access or change.
vi. Raise awareness of computer security and the confidentiality of Commission's data, confidential materials and information amongst management and staff.
vii. Provide guidelines for the proper acquisition and disposal of computer equipment

1.5. GENERAL PRINCIPLES

The Commission's data and/or information and computer systems are assets critical to stakeholders and for execution of the Commission's business. The dependence on these assets demands that appropriate levels of information security be instituted and maintained. The Commission's ICT policy sets appropriate measures to protect its data and computer systems against accidental or malicious destruction, damage, modification or disclosure. The policy will ensure appropriate levels of confidentiality, integrity and availability of such data and/or computer systems. To ensure such compliance, the Commission establishes these general principles:

i. Each component of the Commission's computer system, be it owned, leased, rented, or borrowed by the Commission shall remain under the exclusive control of the Commission
ii. The Commission's computer system and data are critical business assets. Any abuse thereof by any User may render such User liable for disciplinary action in accordance with Commission's Disciplinary Procedures. Users with issues

in relation to this policy and the disciplinary procedures should seek redress with the Executive

Management. In the event that Executive Management fails to resolve the issue, they are entitled to follow the Commission's grievance procedures as prescribed by the Human Resource Policy.

iii. Users may represent the Commission in their dealings with the outside world and use Commission's computer system or data. These systems and data may carry identification of the Commission and may not only reflect the name and reputation of the Commission but may also possibly bind the Commission. This may involve certain obligations and/or liability on behalf of the Commission and/or the User.

iv. It is therefore every User's duty to use the Commission's computer system and data responsibly, professionally, ethically, and lawfully. Users should endeavor to promote and ensure the confidentiality, integrity and availability of the data.

v. Use of the Commission's computer system is provided primarily to assist Users in the performance of their work for, and on behalf of the Commission. The Commission recognizes limited personal usage in terms of this policy as its absolute discretion and that no User may expect or claim this personal use as a right.

vi. The User accepts that the access, review and monitoring of user-activities will be performed by the Commission.

1.6. POLICY MAINTENANCE

Supporting standards, guidelines and procedures will be issued as and when necessary by the Chief Executive of FC in conjunction with the ICT Department. Users will be informed of any subsequent changes or updated versions of such standards, guidelines and procedures. Users shall then have the obligation to obtain the current ICT Policy from the Commission's intranet or other relevant communication media on an ongoing basis and accept the terms and conditions therein.

All users are required to acknowledge receipt and understanding of the guidelines contained in this document.

SECTION TWO

2.1. ICT ACCEPTABLE USE

2.1.1. Access Control

Access Control ensures that accurate identification of authorized members provides secure authenticated access to, and use of all computer systems and services which is to be put in place. The Commission's Access Control Strategy includes secure and accountable means of authorization and authentication.

Authorization is the process of determining whether or not an identified individual or class of individuals have been granted access rights to an information resource and determining what type of access is allowed, e.g., read-only, create, delete, and/or modify.

Authentication is the process of confirming that a known individual is correctly associated with a given electronic credential, for example, by use of passwords to confirm correct association with a user or account name.

2.1.2. Access Control Strategy

The major provisions in the Access Control Strategy are:

i. Access to the network, servers and other systems (eg. routers, PDA, GPS, etc) should require authentication by unique logins.
ii. Access to computers, software applications, and electronic information should be through User identifiers (user name, finger prints and facial recognitions) and passwords.
iii. Users are responsible for creating and protecting passwords that grant them access to resources.
iv. User identifiers and passwords must never be shared or displayed to others. All users must secure their username or account, password, and system access from unauthorized use. If Users are given initial passwords they must change their passwords as soon as possible.
v. Users must take steps to protect their desktop and/or laptop computers from unauthorized access by external agents or other FC staff.
vi. Every user of an individual computer is responsible for determining who has access to locally stored data and applications and for managing the appropriate level of access.
vii. Users shall log off from applications, computers, and networks when finished.
viii. Users shall not leave unattended personal computers with open sessions.

ix. It is the ICT Department's responsibility to ensure that security patches (software that fixes security vulnerabilities, often distributed by the vendors of the products) are applied to Users' desktop, laptop or assure that an Information Service Provider installs current patches.
x. Users may only access Commission's computer systems, e-mail and Internet facilities by means of their authorized usernames and passwords.
xi. Users shall not access, or attempt to access, copy, alter or delete the data of any other User
xii. Users shall not access, or attempt to access networks or servers that Users have no legitimate reason to access, whether the Users have the logical access rights to do so or not.
xiii. No employee, may pry into the personal affairs of other Users without a legitimate purpose for accessing their data.
xiv. Users are strictly prohibited from copying the Commission's data for private use.

2.1.3. Password

i. Users shall not knowingly allow the use of their username and/or password by anyone else, whether such other person is an authorized User or not.
ii. Users are alerted to the fact that they are responsible for all work saved or retrieved, messages sent or received, or transactions carried out under their username and password
iii. Passwords are personal and must not be disclosed or lent to others under any circumstances
iv. Passwords shall have a minimum length of eight (8) characters.
v. The use of a combination of letters, numbers and characters is recommended.
vi. If a password is forgotten, the user shall immediately send a request to the ICT Department so that a new password be issued.
vii. Passwords selected by individuals or automatically generated to protect access to information resources should be difficult to ascertain.
viii. Users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents.
ix. Passwords must not be placed in emails unless they have been encrypted.
x. Default passwords on all systems must be changed after installation.
xi. All Users of systems that contain high risk or confidential data must have a strong password that must be changed frequently.

2.1.4. Remote Access

Some personal computer operating systems can be configured to allow access across the Internet and other networks. Individuals must take care to ensure that their systems are configured so as to prevent unauthorized access. Remote access to a particular computer or device on the Commission's network is likely to enable access, (both proper and illicit), to other computers and applications on the network, so more is at stake than the individual's own computers and devices.
Any User requiring access to Commission's data, whilst in any location other than the Commission's Head Office premises, shall obtain the express permission from the Head of ICT Department or his delegated representative under the following conditions:

i. The remote use of Commission's data may only be made available to Users in the performance of their work functions for and on behalf of Commission.
ii. The User further undertakes to protect and safeguard the aforementioned data, in a diligent and conscientious manner.

2.1.5. Systems Administration And Privileged Accounts

The following rules pertain to the use of administrative and privileged accounts:

i. System administrators routinely require access to resources to perform essential system administration functions critical to the continued operation of the resource, however, the number of privileged accounts should be kept to a minimum, and only provided to those personnel whose job duties require them. Use of privileged accounts should be monitored periodically to ensure they are being used for authorized purposes.
ii. Personnel who require privileged accounts should also have non-privileged accounts to use when not performing system administration tasks.
iii. Personnel assigned privileged accounts should be fully informed regarding appropriate access and disclosure of information. Privileged accounts should only be used for authorized purposes. Those assigned the use of privileged accounts should not use their privileges to leak out personal or confidential information relating to others, or to disclose or otherwise use what they may have observed.
iv. Where possible and financially feasible, more than one person must have full rights to any Commission-owned server, storing or transmitting important data.
v. Terminated employees should have their accounts disabled by the ICT Department immediately after termination. Since there could be delays in

reporting changes in user status and responsibilities, periodic user access reviews should be conducted by the ICT department.

vi. Monitoring must be implemented on all systems including recording logon attempts and failures, successful logons and date and time of logon and logoff.

2.1.6. AUTHORIZED USE AND PRIVACY

2.1.6.1. Legitimate Business Use

Use of the Commission's computer system is permitted under the following conditions:

i. Only persons authorized by the Commission as "Users" may access the Commission's computer systems/facilities and only to the extent that such access is required to assist them in the performance of their work.

ii. Any User who is not employed by the Commission shall enter into an agreement, governing the User's relationship with the Commission.

iii. Any person authorizing access to any Commission's data or the computer systems to a User not employed by the Commission, shall ensure that the appropriate agreement has been signed by the User and that it has been accepted by a person at the Commission duly authorized to do so.

2.1.6.2. Limited personal use

Incidental and occasional limited personal use of the Commission's computer system is permitted provided at all times such use does not:

i. Interfere with the User's work or any other User or employee's work or performance.

ii. Interfere with the operation or resources of Commission 's computer system, or

iii. User's further consent to allowing personnel designated by the Head of ICT Department or his delegated representative, to access and review all materials that the User created, stored, sent or received on the Commission's computer system or received through the internet or any other computer network.

2.2. ICT INFRASTRUCTURE SECURITY

2.2.1. Physical Security

The following regulations pertain to physical security:

i. It is the responsibility of every User to ensure that their officially assigned computers and associated peripheral devices are adequately protected

against theft and damage

ii. In the event of the Commission suffering any financial loss as a result of a User's failure to properly protect any Commission's computer equipment, the User may be held accountable for such loss

iii. Should computer equipment be stolen, it must be reported immediately to the Head of Department in writing and copy Administration and ICT, so that appropriate steps be taken, (for example, insurance claims and removal of logical access)

iv. Users shall not permit visitors to gain access to restricted areas

v. Users are responsible for the consequences of permitting people to gain access to restricted areas, and should challenge people without proper identification.

2.2.2. Logical security

Users are responsible for ensuring the security, integrity and confidentiality of all data resident on the hard disk of their personal computers. In addition, to the rules relating to passwords, Users shall take reasonable steps to ensure that confidential materials on their PCs are not:

i. Displayed in their absence

ii. Accessible to unauthorized persons

2.2.3. Computer system maintenance

The ICT Department of Commission shall be responsible for all maintenance and support of computer systems and peripherals. Users must report all ICT related requests for service to the ICT department and Zonal Offices. However, in situations where the Department deems it necessary it may outsource such services.

2.2.3.1. Software usage

The Commission has licensed or developed certain software for use on the Commission computer system. This software is proprietary to the Commission and third parties (Refer to Annex 1). In order to protect its proprietary interests and to ensure compliance with the terms of applicable licenses, Users are prohibited from the following:

i. Copying Commission software for use on any computer other than Commission supplied PC without the written permission of the Head of ICT Department or his delegated representative having the authority to grant

such permission.

ii. Copying or granting access to Commission software for distribution to independent contractors, clients or any third party
iii. Installing or downloading any software other than Commission software onto the Commission's computer system
iv. Modifying, revising or adapting any Commission software
v. Translating, reverse engineering or disassembling of any software resident on the Commission computer system

2.2.4. Data storage and classification

Data created by Users on their computer systems constitutes an asset of the Commission. All Users must classify data according to the categories below. Data classified as sensitive and personal information (as defined below) must be protected during processing, transmission and storage (e.g. using password protected zip files or using encryption mechanisms as defined by the Head of ICT Department or his delegated representative) as provided for by the Data Protection Act, 2012 (Act 843) which protects the privacy of the individual and personal data by regulating the processing of personal information.

2.2.4.1. Sensitive information

i. Client-sensitive information is information relating to a client, which if disclosed to or misused by unauthorized persons, could cause significant harm to the client and thus to the Commission.
ii. Commission-sensitive information is information relating to the Commission that, if disclosed to, or misused by unauthorized persons outside the Commission could cause damage or embarrassment to the Commission. Such information is stored in the Commission's Intranet (***ForestFocus***).

2.2.4.2. Unclassified public information

Unclassified public information is information that is intended to be public and may be made available to any person outside the Commission after obtaining the appropriate permission.
Such information is stored in the Commission's Official Website.

2.3. Anti-virus protection

The connection of the Commission's computers to the World Wide Web exposes these computers to intruders, hackers and viruses. Frequent use of infected pen drives exposes many corporate and personal computers to the threat of viruses. The growth in the number of viruses and the speed with which they spread requires the Commission to take proactive measures to deal with the problem.

2.3.1. Antivirus protection

Computer viruses are software programs that are deliberately designed to interfere with computer operation, delete or corrupt data and multiply itself to other computers. To reduce the impact and prevent the spread of computer viruses, an antivirus must be installed on all the computers on the Commission Network. For continuous protection, the antivirus software will be updated regularly by the ICT Department.

Weaknesses in software released by various software companies are usually corrected through patches. It is therefore important that all laptops and desktops using off-the-shelf software including operating systems must ensure that patches to software packages are carried out as soon as they are available. Many times laptops and desktops which have not had operating systems updated using the latest patches are vulnerable to viruses. Patching must therefore be routine. Commission should ensure that original licensed versions of software are procured to ensure update of patches.

The ICT Department will organize regular seminars to educate the staff of the Commission on ICT security issues and their roles and responsibilities to reduce security threats.

2.3.2. Corporate and bundled centralised antivirus

Corporate versions of antivirus software allow one person in an organisation to manage all computers from a single location. Monitoring from one central computer should be done to find out which computers are up to date and protected and those which are not.
Corporate antivirus products are often the only way to obtain appropriate antivirus software for protecting a server which normally includes anti-spam filtering, anti-spyware, etc at no extra cost.
It is fairly common to find antivirus software preinstalled on new computers.

Bundled antivirus software cannot be centrally managed, and over time different computers in the organisation will be running different antivirus programmes. This makes it harder to manage the computer systems since the ICT staff will need to be familiar with multiple programmes, and renewing several licenses with several companies over the course of a year becomes cumbersome. Antivirus software preinstalled on new computers will be replaced with corporate versions of antivirus software in use by the Commission.

2.3.3. Updates

An antivirus is only as good as its last update. Antivirus software must be automatically updated daily since new viruses appear very regularly. FC must ensure that all computers are hooked to the internet with adequate bandwidth to carry out updates. FC should ensure constant availability of electricity for areas with erratic electric power supply.

2.3.4. Certification

Any antivirus programme chosen for the Commission must be listed on the ICSA *(International Computer Security Association)* Labs List. This shows it has passed tests to find out if it gives adequate protection.

2.3.5. Precautions for users

Users are alerted to the fact that viruses can cause substantial harm to the Commission's computer systems and must therefore note the following precautions:

i. If a virus attack is detected, the Helpdesk serving that Commission's premise should be notified immediately.
ii. Installation of non-Commission approved virus protection software is prohibited
iii. Users are under no circumstances to disable the anti-virus software or re-configure any settings on the anti-virus software unless specifically authorized by the Head of ICT Department or his delegated representative.

2.3.6. Firewalls and computer system security

Firewalls form a major and key component to an enterprise wide security policy and system. Firewalls are designed and deployed to prevent unauthorized access to or from a private network. Both hardware and software implementations are feasible and currently employed by several organizations. The ICT Department must ensure that appropriate firewalls are put in place to protect the network.

2.3.7. Email server

Most viruses these days are transmitted via email. The first line of defence is the email server. The Commission must ensure that the Internet Service provider (ISP) has an effective firewall that checks all emails.

If the Commission decides to host their own e-mail server, then it must ensure that adequate provisions have been made to check viruses by scanning all arriving emails for viruses. The easiest way to obtain this software is part of a corporate antivirus package.

2.3.8. File servers

Servers allow central storage and sharing of files, but sharing must be devoid of viruses. Servers require antivirus software distinct from those specified for laptops and desktop PCs. Furthermore, the acquisition of corporate antivirus packages is the safest remedy.

2.3.9. Personal computers

Every computer in the organisation should have antivirus software installed to protect against pen drive borne viruses. More important is the facility to run scheduled scans to find any infected files in shared and users' folders. Mail servers need antivirus software which check messages as they arrive (and also for spam) and quarantine any infected ones somewhere they can be safely examined.
The use of Commission's email system for non-official related commercial purposes is not allowed. Commission's e-mail system must not be used to send, download, display or store prohibited materials. E-mail containing prohibited material which has been inadvertently received by a User shall be deleted as soon as he or she becomes aware of the content thereof and the incident must be reported to the Head of ICT Department or his delegated representative without delay.

2.4. Transmission of confidential material

Confidential materials shall not be sent, transmitted or otherwise disseminated by Users to third parties unless the User has satisfied himself/herself that:

i. He/she is duly authorized to send, transmit or otherwise disseminate the relevant confidential material, and it is in the ordinary course of the business of the Commission or in the Commission's best interest to send, transmit or otherwise disseminate such confidential material, and that
ii. Such confidential materials are already in the public domain, or
iii. The intended recipient is entitled to receive such confidential materials.
iv. For formal confidential correspondence: mails should be encrypted or password protected before sending. Passwords and encryption codes should not go with the same mail.

2.5. Retention of data including e-mail

Email correspondence and electronic material belonging to FC is subject to same retention policies covering printed documents. Users are required to ensure that all data that may be required to be retained by relevant legislation such as the Commission's Document

Retention Policies and the Data Protection Act, 2012 (Act 843) passed by Parliament as part of the laws developed under the Information and Communications Technology for Accelerated Development (ICT4AD) Policy that seeks to create an enabling legal environment for the development and use of ICT in the country.

2.6. DISCLOSURE

2.6.1. Internal Disclosure

The contents of legitimate business e-mail may be disclosed within the Commission without the permission of any User who was the addressor or addressee of such e-mail. However, any internal disclosure within the Commission without the consent of the Users concerned shall be limited to those users or employees who have a reasonable need for access to such e-mail.

2.6.2. External disclosure

Commission may in its discretion and for any legitimate purpose, disclose to third parties the contents of e-mail messages sent to, or received by it's Users. The Commission will, however, attempt to accommodate any objections to such disclosure on the following grounds, reasonably based:

i. That such disclosure will create personal embarrassment for the User concerned, unless such disclosure, in the Commission's discretion, is required to serve an important business purpose or satisfy a legal obligation.
ii. That the contents of such message are personal and private in nature and that Commission is not under any legal obligation to make such disclosure.

2.6.3. Disclosure of data contained in e-mail for legal purposes

If Commission is legally obliged to disclose e-mail messages to a third party, the Commission shall give reasonable prior notice to the User whose e-mail is required to be disclosed, unless:

i. Commission is legally obliged to allow such disclosure without reasonable notice or without any notice at all, or
ii. Such disclosure is required by a law enforcement agency, and
iii. It is contrary to the interests of justice or law enforcement to notify the User of such disclosure, or
iv. No User shall of his or her own accord, respond in any way to notice or demand to disclose any particulars with regard to FC or to any subpoena to produce an e-mail at any court proceedings, (other than to acknowledge receipt thereof if necessary) without first obtaining the authority and advice of the Head of the Legal Department, or someone authorized by him or her in writing.

SECTION THREE

3.1. INTERNET AND EMAIL USAGE

3.1.1. Purpose

The purpose of this policy is to ensure that staff of the Commission properly use the email and Internet communications systems for their intended purposes. The use of **email** and **Internet** by staff is permitted and forms part of the normal execution of an employee's job responsibilities. Its use is encouraged where it is suitable for business purposes and in a manner that is consistent with the Commission's standards of business conduct. The personal use of email and the Internet is occasionally accepted. However, the usage of the Commission's domain name to conduct personal business other than official business is prohibited.

3.1.2. Use of Internet Guidelines

Use of the Internet in the following manner is strictly prohibited:

i. Using Internet access provided by FC to conduct any other business than that of the Commission, including hosting or displaying personal web pages
ii. Subscribing to or participating in chat groups, bulletin boards, newsgroups, or discussion groups (e.g. Social sites like Facebook, LinkedIn, Twitter, Chatting rooms, etc.) that are not business related
iii. Browsing the Internet for non-business purposes during official hours
iv. Using or posting sensitive and personal information while accessing the Internet, (including but not limited to username, passwords, security codes or server-specific information) which could assist third parties in gaining unauthorized access to the Commission's computer system.
v. Publishing or transmitting Commission's data of a confidential nature on or via the Internet. If a situation exists where confidential material has to be transmitted, written authorization will be required by the appropriate authority, prior to the transmission or publication of such information on or via the Internet. If such authorization is conditional, then all conditions shall be met before transmitting the confidential material.
vi. Staff must not participate in any online activities that are likely to bring the Commission into disrepute, create or transmit material that might be defamatory or incur liability on the part of the Commission, or adversely impact on the image of the commission.
vii. Staff must not visit, view or download any material from an internet site

which contains illegal or inappropriate material. This includes, but not limited to, pornography, obscene matter, race hate material, violence condoning message, criminal skills, terrorism, cults, gambling and illegal drugs.

viii. Staff must not knowingly introduce any form of computer virus into the Commission's Local Area Network.

ix. Staff must not download commercial software or any copyrighted materials belonging to third parties, unless such downloads are or permitted under a commercial agreement or other such licence.

x. Staff must not use the Internet for personal financial gain.

xi. Staff must not use the Internet for illegal or criminal activities such as, but not limited to, software and music piracy, terrorism, fraud, or the sale of illegal drugs.

xii. Staff must not use the internet to send defamatory, offensive or harassing material to other users.

xiii. Visit to and use of gambling sites is not permissible.

xiv. Staff shall face disciplinary action or other sanctions if they breach this policy and or bring it into disrepute.

xv. Family members, friends, relatives and other unauthorized persons must not have access to the Commission's internet facilities.

3.1.3. Use of email guidelines

Users of the email system should follow these guidelines and conventions:

i. Ensure that messages are addressed to the appropriate recipient

ii. Cover periods of absence by adopting an appropriate functional account forward, or vacation message strategy.

iii. Use of the email system in the following manner is strictly prohibited.

   a. The creation and exchange of messages that are offensive, harassing, obscene or threatening.

   b. The exchange of proprietary information, trade secrets, or any other privileged, confidential or sensitive information outside the Commission, or outside a defined privileged group.

   c. The creation and exchange of official advertisements, solicitations, chain letters and other unsolicited email.

   d. The creation, storage or exchange of information in violation of copyright laws.

   e. Altering or copying a message or attachment belonging to another user without the permission of the originator.

3.2. Addressing electronic mail

Email addresses within this Commission shall adopt the following standard format for all staff:

i. **first letter of** firstname + surname.(division)@fcghana.org
ii. In exceptional cases where a duplicate name exists, system administrators should be called upon to ensure appropriate email address is issued. An email address shall be created for external partners e.g. tourists, researchers, etc. to communicate with the Commission. This address shall be the address published on Commission's Intranet and other notice boards and shall follow the same format.

3.2.1. Non-personal Division Email Addresses

The following non-personal email addresses shall be created for various units:
info.division@fcghana.org – for the division (HQ, FSD, WD, TIDD, RMSC, FCTC)

3.2.2. Formal Correspondence And Other Documents

i. All official meetings in the Commission should be communicated through the corporate email system. Any formal document of FC which any staff wishes to transmit via e-mail, shall be sent as an attachment to an e-mail message on the Commission's letterhead template provided for this purpose or other formal correspondence material.
ii. Users are alerted to the fact that email communications can bind FC to an agreement and users need to comply with the relevant statutory requirements and Commission's policies as communicated to them in this regard. If the staff is in any doubt, clarification should be obtained from the Head of ICT Department or his delegated representatives.
iii. All e-mail communications are Commission's records, Commission reserves the right in its discretion to access and disclose all legitimate business communications sent using Commission's e-mail system.

3.2.3. Misaddressed E-mail

Misaddressed e-mail that may have been received and opened inadvertently must be deleted from the Commission's computer system immediately by the User receiving and opening such e-mail.

3.2.4. E-mail Procedures For Retirement

Since the corporate E-mail System is intended for official correspondence only, the Head of the Human Resources Department or his/her representatives should submit to the Head of ICT or his/her representatives, the list of all personnel 3 months prior to retirement to enable the ICT Department configure all e-mail account details with due dates for all the affected staff for deactivation.

3.2.5. E-mail Procedures For Termination/demise

The Head of Human Resources Department or his/her representatives should inform the Head of ICT or his/her representatives immediately personnel appointments have been terminated or have passed away during active service to enable the ICT Department reconfigure their e-mail account details.

3.1. Monitoring

Commission's computer system is provided to staff for use in the promotion of Commission's business and incidentally for personal purposes. In order to protect its rights and interests, FC reserves the right to access and read the contents of e-mail messages and track Internet usage in the following circumstances provided that, subject to the restrictions set out below, FC will not seek to obtain access to the contents of any User's e-mail files without the permission of the User concerned:

i. If it is required by law or by legal obligations to third parties to do so
ii. If there is a legitimate business need or reason to do so (e.g. when traffic monitoring is not sufficient to establish violation of this policy or any relevant legislation)
iii. In the event that there is sufficient reason to suspect that a User has committed or is committing a crime that might be aimed at the Commission, or in respect of which the Commission may incur any liability; criminal or financial.
iv. If it is of bona fide opinion that such access or disclosure may be necessary to investigate a breach of security of the e-mail system.
v. Should the Head of ICT Department or his delegated representative encounter indications of illegal activity or violations of ICT policy or security, he/she shall investigate further and report any findings to the head of the department concerned

SECTION FOUR

4.1. EQUIPMENT DISPOSAL

4.1.1. Introduction

Computer equipment may not be required for various reasons such as:

i. Exceeded useful lifespan
ii. Obsolescence
iii. No longer utilized
iv. Damaged
v. Excessive cost of maintenance
vi. Replacement with a newer model
vii. Cost Effectiveness as against Technological Advancement/Demand

4.1.2. Purpose

The purpose of this policy is to establish and define standards, procedures, and restrictions for the disposal of computer equipment in a legal, environmentally friendly and cost-effective manner. The Commission's surplus or obsolete ICT equipment (i.e. laptops, desktop and handheld computers, servers, UPS, LCD projectors, etc.) must be disposed of according to legal requirements and environmental regulations of the country. All disposal procedures for retired computer equipment must adhere to Commission's approved methods and authorization granted by the Chief Executive through the Head of Finance & Administration Department and the Head of ICT Department.

4.1.3. Scope

This policy applies to the appropriate disposal of all Commission's equipment including PCs workstations, laptops, servers, switches, routers, hand-held devices, printers, scanners, LCD projectors and so on. Commission-owned surplus equipment, obsolete equipment, and any equipment beyond reasonable repair or reuse are covered by this policy. Where applicable, it is desirable to achieve some residual value of the equipment in question through reselling, auctioning, donation, or reassignment to a less-critical function.

4.1.4. Guidelines For Disposal

Disposal of computer equipment shall be guided by the following principles:

i. Disposal or re-assignment of all computer equipment which is the property of the Commission, no matter what the original funding source, will be the responsibility of ICT Department.
ii. The ICT Department must be notified to pick up the equipment in writing. The Equipment Disposal Form (Refer to Annex 2) must be completed before disposal.
iii. Disposal of surplus computer equipment will follow the relevant provisions in the Public Procurement (Amendment) 2016 (Act 914) and existing financial policy of the Forestry Commission.
iv. Before an equipment is considered for disposal, the user or requester shall contact ICT Department to determine the usability or otherwise per the Lifespan of ICT Equipment (Please refer to Annex 4) which is based on IS0 standards and best practice.
v. When disposing of computer equipment, any file on disk which contain personal, sensitive or confidential data must be deleted such that it cannot be recovered by anyone. E.g. Old PCs may normally be disposed of to a third party with the original Operating System installed. However any Microsoft Office products for example must be removed in order to fulfil the licensing conditions.
vi. Hard Disks and any other storage media should be removed from the equipment before it is disposed off.
vii. CD's, flash/pen drives, etc. should be burnt, baked, or crushed before disposal.

4.1.5. Acceptable Methods For Disposal

Acceptable methods for the disposal of Computer equipment are as follows:

i. Used as a trade-in against cost or negotiated discount rate of replacement or associated item. This option is only available for some repairers and Second-Hand PC vendors.
ii. Sold by auction or by a third party
iii. Donated to schools, charities and other non-profit organizations.
iv. Disposed off in accordance with the relevant legal and environment laws of Ghana. It is the responsibility of any employee of the Commission with the appropriate authority to ensure that Computer equipment is disposed off

according to one or more of the methods prescribed above. It is imperative that any disposal performed by the Commission are done appropriately, responsibly, and ethically. The following rules must therefore be observed:

a. Equipment sold or given to Staff: Any equipment sold or given to staff must not be reemployed for sanctioned use at the Commission. Such equipment is not supplied with any additional software and data other than the operating system and freely available software. Technical support is not available for such equipment.
b. Trade-Ins: Where applicable, in cases where a piece of equipment is due for replacement by a newer model, reasonable actions must be taken to ensure that a fair and market trade-in value is obtained for the old equipment against the cost of the replacement. The Head of ICT Department or his/her representatives will assume this responsibility.
c. Donations: Computer equipment may be donated to a Commission-approved school, charity, or other non-profit organizations. All donations must be authorized by the Chief Executive.
d. Cannibalization of Equipment beyond Reasonable Repair: The Head of ICT Department is responsible for verifying and classifying any equipment beyond reasonable repair. Equipment identified as such should be cannibalized for any spare and/or working parts that can still be put to sufficient use within the Commission. The ICT Department will inventory (stockpile) these parts. The remaining parts and/or whole machines unfit for use or any other disposal means will be disposed accordingly
e. Decommissioning of Equipment: All hardware slated for disposal by any means must be fully wiped clean of all Commission's data and software. ICT Department will assume responsibility for decommissioning this equipment by deleting all files.
f. Income Derived from Disposal: All receipts from the sale of the equipment must be accounted for and remitted to the Finance and Administration Department of the Commission.
g. All disposal methods including donations must be approved by the Chief Executive.

SECTION FIVE

5.1. ICT EQUIPMENT ACQUISITION

5.1.1. Introduction

This policy provides guidelines for acquisition. It will also help to reduce total cost of ownership and to realize efficiencies in operations. Minimum specifications and standards must be set for all ICT equipment to be acquired in the future. Some of the benefits of implementation of this policy will be:

i. Defined minimum standards and specifications for all ICT equipment
ii. Faster support resolution for problems.
iii. Reduced maintenance requirements and support cost.
iv. Defined and streamlined procedures for acquisition of ICT equipment.
v. Reduction in errors in ordering and configuring.
vi. Cost savings through coordinated ICT equipment acquisition and also best use of ICT equipment budget.

5.1.2. Purpose

The purpose of the FC ICT equipment Acquisition Policy is to provide:

i. Acquisition procedures for Desktops, Laptops, handhelds, printers, scanners, LCD projectors etc.
ii. Minimum specification and configuration standards for procuring ICT equipment.

5.1.3. Scope

This policy applies to all ICT equipment purchases made (in whole or in part) with Commission funds that are intended for use by staff and affiliates of Commission.

5.1.4. Strategy

Computers will be delivered pre-installed with necessary licensed software to the Commission's stores. Once the computers have been delivered and received into the stores, they will be delivered to the ICT Department. The ICT Department will then setup and configure user accounts, and install any additional software as may be required, and join to FC's domain for security reasons where necessary. The ICT

equipment will then be delivered to the user Departments.

5.1.5. Donor-funded Equipment

Donor funds received by the Commission which require the purchase of ICT equipment, shall adhere to this policy. Since Donor-funded equipment eventually becomes the property of Commission after the project completion; it is essential that this equipment follow the same procedures and standards as those procured with the Commission's funds.

5.1.6. Exemptions And Waivers

Any work demand which requires a specialised equipment other than the standard equipment should be approved by the Chief Executive.

5.1.7. Guidelines On Ict Equipment Allocation

i. A staff shall not be assigned more than one laptop or desktop computer.
ii. All project ICT Equipment are the properties of FC. Staff shall not possess one FC funded laptop or desktop computer and another project funded laptop or desktop computer at the same time and one shall be reassigned for optimised use of resources by the Commission.
iii. Staff shall not install non-official software on any FC ICT Equipment
iv. All FC Official Software (Refer to Annex 1) should be installed by the ICT Department or with the prior approval by the Head of ICT Department
v. All ICT Equipment should be officially labelled.

5.1.8. Loss of ICT Equipment

Staff shall report to the police station and submit a police report in all cases of loss involving ICT equipment. Police investigation report(s) and internal investigation report(s) shall be the basis for sanctions where appropriate.

5.1.9. Damaged ICT Equipment

i. The ICT Department to conduct Technical Assessment in all cases to ascertain the degree of damage and submit report in writing to the Chief Executive.
ii. FC will repair or replace ICT equipment based on the outcome of assessment conducted.

iii. Where the technical assessment report indicates the user of negligence, appropriate sanctions shall be applied.

5.1.10. FAULTY ICT EQUIPMENT

i. All faulty ICT Equipment shall be sent to the ICT Department (FCHQ, TIDD, FCTC, RMSC and ICT Zonal Offices) for technical assessment, the outcome of which will determine whether it will be repaired internally or externally.
ii. For internal repairs, a jobcard will be prepared and where appropriate a request sent to Finance Department for funds to purchase faulty parts before repair is undertaken.
iii. For external repairs, a waybill will be prepared for onward submission to Service Providers, especially ICT Equipment which are under warranty or where external expertise is required.
iv. Failure to follow the above procedures will result in non-payment of repair works.

SECTION SIX

6.1. DATA ADMINISTRATION AND SOFTWARE APPLICATION DEVELOPMENT

6.1.1. Introduction

The Forestry Commission recognizes data as an institutional asset and resource vital to the strategic and operational processes within the Commission. Data differ from traditional assets in many ways, and the costs associated with inadequate or incorrect data are frequently hidden. Unlike other assets, data can be copied and used several times, and are not always assigned a monetary value. However, insufficient or inaccurate data can adversely affect all aspects of the Commission resulting in huge costs.

Examples of such costs include: maintenance and development costs associated with duplicate databases and applications, and costs resulting from poor management decisions based on bad or inadequate data.

Data must be managed as any other asset, and the Commission has a responsibility to improve the efficiency of processes associated with the collection, storage, maintenance, processing, analysis, reproduction and presentation of data, as well as ensuring adequate data access while maintaining necessary levels of security and privacy. While Commission owns the data, various Divisions within the Commission have stewardship responsibilities for subsets of the data. Consequently, the Commission must approach data management in a comprehensive and systematic fashion, where its responsibility is shared by all. In the light of the above, there is the need for this ICT Policy to ensure effective data administration and software application development.

6.1.2. Purpose

The purpose of the policy is to:

i. Guide all software application development and acquisition in the Commission
ii. Establish the principles guiding the effective management of information and data.
iii. Ensure that only authorized users have access to Commission's computer-based data and information
iv. Prevent misuse, loss, or destruction of computer-based data and information
v. Ensure compliance of the procedures for gaining access to the Commission's applications and databases and the requirements for proper use and

protection.

6.1.3. Scope

This policy applies to:

i. Authorized FC employees involved in data and information management activities as well as the use of the Commission's data and ICT infrastructure.
ii. Authorized FC employees involved in the engagement of third parties in the acquisition of off-the-shelf as well as developed software applications
iii. Authorized stakeholders involved in our data and information management activities.
iv. The general public who may be given access to the Commission's information and data.

6.1.4. Data Architecture

The Commission shall utilize Data/Information Architecture target technologies, methodologies, standards, and best practices to develop, acquire, and/or implement application systems that collect, modify, store and process data and report information.

6.1.5. Data Formats

The Commission shall utilize Data/Information in various formats where applicable. The various formats shall cover digitized documents, maps, correspondence, documentations, etc and e-archived accordingly.

6.1.6. Data Usage

This policy is intended to ensure that the data assets of the Commission are not misused or abused. The use of data falls into three (3) categories, namely read-only, update and external dissemination. The ICT Department shall grant authority to update data only to personnel whose job duties specify responsibility for data update. This restriction is not to be interpreted as a mandate to limit update authority to members of any specific group or office.

6.1.7. Data Access

Open access to data and information will be provided to the Commission's staff for the support of the Commission's functions. A default access is defined as Open Access to all employees. In contrast, Restricted Access limits information to all others except for information designated as part of the "public record."

6.1.8. Data Access Control

Access Controls should provide reasonable assurance that data and applications are protected against unauthorized use, modifications, disclosure, loss or destruction. These controls include physical controls, such as keeping a computer under lock and key to limit physical access, and logical controls such as security software programs designed to prevent or detect unauthorized access to sensitive files/data.

Security software provides a means of specifying who has access to a system, who has access to specific resources, and what capabilities authorized users are granted. Data users must take note of where files are maintained and archived, and understand when and how to delete them.

All persons other than authorized ICT staff shall put off their electronic gadgets before accessing restricted ICT facilities.

6.1.9. Data Management

The quality and veracity of Commission's decisions are directly related to the quality of the data on which those decisions are based. Thus, the Commission's data shall be planned for, collected, processed, managed and protected as the valuable resources they represent.

The collection, processing, storage and dissemination of the Commission's data will be guided by the following principles:

i. The management of the Commission's data will be based on best practices and standards in information management, and the value of our data will not be compromised.

ii. The collection, validation, storage and dissemination of data depend on individuals, however, the data is owned by the Commission.

iii. Each data programme will have documented procedures for reporting and correcting data errors, and emphasis will be placed on identifying and eliminating data errors at their source.

iv. Data quality will be managed through clearly defined and documented roles and responsibilities of the designated staff of the Commission. The individual or group that has the greatest vested interest in the quality of the data will have the greatest responsibility to ensure the quality and integrity of that data.

v. The Commission will promote and facilitate the sharing and exchange of information and data, within and outside the Commission, through the use of

data and information management plans, protocols, guidelines and standards.

vi. The data and information resources and reporting requirements will be catalogued along with formal and comprehensive metadata in a data registry which will be complete, current, and searchable within and outside the Commission.

vii. The data and information products and reports will be derived from a single data source that is legally verifiable through the use of formal methods for user auditing, data change management and access security.

viii. Data will be both available and accessible to all appropriate users, in a timely and efficient manner.

6.1.10. Data Backup

All critical Commission data must be backed up on a regular basis. Frequency of backup is determined by the frequency with which the data changes and the effort required to recreate the information if lost. A maximum of seven (7) days data backup interval is required.

i. Information stored on any Commission's servers shall generally be backed up automatically, following established procedures for off-site storage and business continuity readiness.

ii. It is mandatory for users to store important files on these servers.

iii. The ICT Department shall ensure that regular backup copies are made of mission critical data and maintained in a different physical location to protect against disk failure, virus, malicious activity, accidental deletion and other catastrophes such as fires and floods.

iv. The Commission shall establish and maintain a Disaster Recovery Site (DRS) in RMSC, Kumasi to ensure real-time redundancy of the Commission's ICT services.

v. ICT Department must take care to store electronic media under environmentally appropriate conditions. Because electronic media can degrade under any condition, copies that may require long-term retention shall be periodically refreshed, tested and documented by the ICT department.

vi. Staff shall comply to ICT backup directives concerning official data storage on their client equipment (computers, laptops, handheld devices, ipads etc).

vii. Staff should be trained on how to backup their data on daily basis whilst the ICT Department undertakes continuous and periodic backups.

6.1.11. Data Retention

Custodians of the Commission's data are responsible for defining and documenting the length of time data must be retained. The retention period, legal requirements, responsible parties, and source of legal requirement should be documented. (Refer to Annex 5).

6.2. Software Application Development

All software application development request in the format as prescribed in the Software Request Form (Refer to Annex 6) shall be submitted first to the Head of the ICT Department for the necessary attention. The request will include the Terms of Reference (ToR) by providing the objectives, and a brief on the inputs (information and users), the scope, and output (types of reports) of the proposed application.
The Head of ICT department will recommend to the Chief Executive for approval for the appropriate application:

a. In-house
b. Off-the-Shelf
c. Development by external parties.

Having regard to Systems Development Lifecycle, a Terms of reference, a user and technical specification as agreed by both parties and signed-off accordingly before commencement.

6.2.1. Minimum Conditions/procedures

All software applications (in-house, off-the-shelf and external) must ensure that the following minimum conditions/procedures are met:

6.2.2. Security

i. Authentication of individual users and not groups.
ii. Stored passwords should be encrypted and not stored in clear text or in any easily readable form.
iii. Provide role management, such that one user can take over the functions of another without having to know the other's security credentials especially password.
iv. Audit trail reports for tracking activities of users

6.2.3. Mode Of Operation

On-line and off-line modes for web-based applications to ensure that there is real-time data irrespective of interruptions of internet service.

6.2.4. Source Codes

All associated source codes of the applications should be the bonafide property of the Forestry Commission in all circumstances.

SECTION SEVEN

7.1. ICT TRAINING

7.1.1. Purpose

The fast changing landscape of ICT requires the constant need to upgrade one's skills and knowledge. The purpose of ICT training is to equip all staff of the Commission with the necessary skills, knowledge and attitudes to meet the Forestry Commission's needs in relation to its objectives and that of its stakeholders.

The Commission recognizes the potential for ICT in its various applications to increase productivity as well as improve the efficiency, effectiveness and capabilities of various Divisions, Departments and Units. The implementation of these applications requires building the capacity of staff in the adoption and utilisation of state-of-the-art technologies.

By investing in staff training, the Commission will ensure that the full potential of the employees are harnessed to fulfil their need for personal development and job satisfaction. The Commission recognises that ICT training is a continuous process for every employee at every level of the organisation. ICT training is a necessary investment in order to provide the excellent services the Commission demands.

7.1.2. Training Needs Assessment

The Training Needs Assessment (TNA) takes cognisance of the need to develop an effective training programme which aligns with the overall vision, mission and goals of the Commission. The TNA is a process of identifying the "gap" between the technology awareness, knowledge and skills of the staff and the requisite level of ICT knowledge and skills required for the successful performance of an employee's work.

The variance between the desired and the actual levels would determine the content of the training programme. It will also affect the actual training that will be required. Taking cognisance of the different levels of ICT maturity among the staff, the TNA will aim at producing a balanced competency-based, responsive and demand-driven training programme.

The key benefits of this include but not limited to the following:

i. Assessment of the staff's knowledge and skills in ICT in general
ii. Assistance in identifying the specific areas of ICT applications to use in the training

iii. Provision of data to support specific training content

7.1.3. Types of Training Required for ICT Users

Staff of the Commission use the computer on daily basis for their work and requires training on the following:

i. Business Application Software (Accounting software, Forest Management system, Human Resource Management system, etc.)
ii. MS Office Applications (Word, Excel, Power Point, Visio, Access, Outlook, Project, Publisher, etc.)
iii. Newly acquired software application by the Commission.

7.1.3.1. TRAINING FOR ICT PROFESSIONALS

There will be a need to train qualified staff to manage the ICT infrastructure at the Commission. All the ICT staff must participate in regular training sessions in order to remain current on the fast and continuously changing landscape of ICT. There is a wide spectrum of courses available for ICT professionals. These include:

i. Computer Hardware & Network Maintenance and Support
ii. Systems Administration Support (Network Monitoring and Management Tools)
iii. System Security
iv. Data Communication
v. Support for Business Application Software packages
vi. Software Development (Web Technology)
vii. Mobile Devices and Applications
viii. General Support and Assistance to FC staff (Client Service Management)

7.1.3.2. TRAINING RESOURCES

The Commission will ensure that financial resources and logistics required to meet ICT training needs are fully identified and provided.

7.1.4. TRAINING METHODS

There are several ways of approaching training. The following methods should be considered:

7.1.4.1. Formal Classroom Training

Formal classroom courses provide consistency, and ensure that all the necessary elements of a syllabus are adequately covered.

7.1.4.2. Computer-based Training

This can be provided either on CD-ROM, pendrive or online, allowing automatic monitoring of the learning process. Several ICT courses are easily available online as affordable modules that one can undertake and finish in 2 weeks or to a year. Some of the online courses are free. For example, Microsoft offers a free digital literacy program skills including computing, internet, office applications based on the Microsoft product range. Also free online training on the use of Microsoft Office Products are available. In addition there are other online courses including those available on the OpenOffice.org support site.

Webinars are another option and allow participants to ask questions directly to the speaker, and hear the questions and answers given by others. One can often download audio or view video at a later date, and listen or watch later. Several organisations offer a lot of free webinars on ICT topics.

SECTION EIGHT

8.1. ENFORCEMENT AND DISCIPLINARY ACTIONS

8.1.1. Introduction

An ICT Policy breach is defined as any action or event in contravention to the provisions of this ICT Policy. All users of the Commission's computer system have the responsibility to report any apparent violations of the ICT Policy whenever such violations come to their attention by using existing reporting lines.

Violations of this policy will be handled in accordance with FC's policy on disciplinary actions, where offences are classified as Minor, Major and Intolerable and specifcally in refernce to ICT, the classifcation is as provided in Annex 3. The Commission may temporarily suspend, block or restrict access to information and network resources when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of the Commission's ICT resources or to protect the Commission from liability.

A User who contravenes the terms and conditions of this policy acknowledges that he or she will be acting outside of the course and scope of his or her employment, or his or her contractual obligations to the Commission. With regard to a non-employee User of Commission's computer systems, such User shall be obliged to enter into a written agreement with Commission which shall expressly prohibit any contravention of this policy.

8.1.2. Security Breach Notification & Reporting

Any person who identifies a security breach should notify the Head of ICT Department or his/her delegated representative. A technical investigation of the security breach must be carried out and a report submitted outlining the following details (where appropriate):

i. General nature of the security breach;
ii. List of people involved in the security breach,
iii. Computer systems involved in the security breach;
iv. Details of the security breach;
v. Impact of the security breach;
vi. Potential consequences of the security breach;
vii. Possible courses of action to prevent a repetition of the security breach;

8.1.3. Enforcement

Any person who violates any portion of this policy;
Shall be dealt with in accordance with FCs policy on disciplinary actions. May expose themselves personally to claims for damages for wrongful infringement of privacy rights, or May be liable to criminal prosecution.

i. In situations where the violation involves suspected criminal activities, the Commission may refer the matter to the appropriate law enforcement agencies.
ii. The Commission may monitor network traffic for the detection of unauthorized activity and intrusion attempts, view or scan any file or software stored on the Commission's systems or transmitted over the Commission's networks.

8.1.4. Relaxation And Waiver

Failure of the Commission to take action in conformity with this policy or to require performance of any provision of this policy shall not affect the right of the Commission to require performance of that provision or of any other provision in the future. No waiver by the Commission with respect to a breach of any provision of this policy shall be construed as a waiver with respect to any continuing or subsequent breach of that provision, or as a waiver of any other right under this policy.

SECTION NINE

9.1. POLICY IMPLEMENTATION

9.1.1. Introduction

The ICT Policy Implementation is the process of turning policy into practice. In order to implement this policy, certain conditions must be in place for policy implementation to be effective. These include but not limited to:

9.1.2. Conditions For Successful Implementation

i. Set date for launching the policy. The policy comes into effect from that date. Create awareness among employees. At the launch of the policy, copies (manual/electronic) must be made available to all employees. All newly recruited staff must be made aware of the existence of such a policy.
ii. At staff meetings policy issues should be highlighted when agenda items are related to the policy
iii. Get senior management to be committed to the policy implementation. This will ensure successful implementation of the policy
iv. Clearly document sanctions for violations. This must be consistent with the Human Resource policy of the Commission on disciplinary actions for employees
v. Make available adequate and sufficient resources for successful implementation
vi. Institute measures to remove barriers to implementation
vii. Policy must be reviewed biennially and changes brought to the attention of all staff. In reviewing policies the inputs of all stakeholders must be solicited and considered for inclusion if relevant.

9.1.3. ICT Equipment

With the adoption of this policy, the Procurement Unit of FC will ensure that acquisitions of all ICT equipment conform with specifications determined by the ICT Department. The ICT department will install, configure, support, or repair all FC computer equipment.

9.2. ROLES AND RESPONSIBILITIES

9.2.1. Implementation Plan

i. The ICT Department is responsible for publication of policies and standards, the provision of advice and guidance, monitoring compliance, and the co-ordination of efforts required to attain the policy objectives.
ii. The ICT Department will report major incidents or threats which adversely affect the continued operation of ICT systems of the Commission to the Executive Management Team.
iii. The ICT Department will coordinate with the Human Resource Department to determine the sanctions for violations in accordance with the existing HR Policies of the Commission
iv. The ICT Department will set milestones and deadlines for the implementation of the Policy.

9.2.2. Management Responsibilities

The overall responsibility for ICT governance rests with the Executive Management Team of the Commission and requires that appropriate ICT policy measures be introduced and observed by all Users of the Commission's computer systems. The management of Commission is responsible for ensuring that good security practices are implemented and maintained within their area of responsibility by:

i. Ensuring Users know what is expected of them and that they act in an acceptable way to protect Commission's data and information systems.
ii. Ensuring that standards and procedures are followed correctly at all times.
iii. Maintaining an appreciation of the risks associated with the loss of confidentiality, integrity or availability of information and ensuring that where adequate standards and procedures are missing, an appropriate person is notified for action.
iv. Setting a good example to Users by taking the lead in applying good security principles to their own work.

GLOSSARY

Access point: A device that allows wireless-equipped computers and other devices to communicate with a wired network.

Address: Identifies the location of an Internet resource. Examples: an e-mail address (info.hq@fcghana.org); a web address (http://www.fcghana.org); or an internet address (192.168.100.1).

Application: A program designed for a specific purpose, such as word processing or graphic design.

Attachment: A file that is sent along with an e-mail message.

Authentication: The process of identifying yourself and the verification that you're who you say you are. Computers where restricted information is stored may require you to enter your username and password to gain access.

Bandwidth: A measurement of the amount of data that can be transmitted over a network at any given time. The higher the network's bandwidth, the greater the volume of data that can be transmitted.

Bluetooth: A wireless networking technology that allows users to send voice and data from one electronic device to another via radio waves.

Browser: A program used to access World Wide Web pages. Examples: Firefox, Safari or Internet Explorer.

Cache: A region of computer memory where frequently accessed data can be stored for rapid access. The act of storing data for fast retrieval is called "caching".

Case-sensitive: Generally applies to a data input field; a case-sensitive restriction means lower-case letters are not equivalent to the same letters in upper-case. Example: "data" is not recognized as being the same word as "Data" or "DATA".

Client-server: Refers to a connection between networked computers in which the services of one computer (the server) are requested by the other (the client). Information obtained is then processed locally on the client computer.

Courseware: Software designed specifically for use in a classroom or other educational setting.

Database: A collection of information organized so that a computer application can quickly access selected information; it can be thought of as an electronic filing system. Traditional databases are organized by fields, records (a complete set of fields), and files (a collection of records).

Desktop: On computers like IBM PC or compatibles and Macintoshes, the backdrop where windows and icons for disks and applications reside.

Disaster recovery: Disaster recovery is the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster. Disaster recovery is a subset of business continuity. While business continuity involves planning for keeping all aspects of a business functioning in the midst of disruptive events, disaster recovery focuses on the IT or technology systems that support business functions.

E-mail: Electronic mail; the exchange of messages between users who have access to either the same system or who are connected via a network (often the Internet). If a user is not logged on when a new message arrives, it is stored for later retrieval.

Encryption: The manipulation of data to prevent accurate interpretation by all but those for whom the data is intended.

External User Any person (either FC Staff or Non-FC Staff) aside the authorized user of a specific application/computer/laptop is an external agent.

File: A collection of data that has a name (called the filename). Almost all information on a computer is stored in some type of file. Examples: data file (contains data such as a group of records).

Firewall: A method of preventing unauthorized access to or from a particular network; firewalls can be implemented in both hardware and software, or both.

Flash drive: A small device that plugs into computer's USB port and functions as a portable hard drive.

Flash memory: A type of memory that retains information even after power is turned off; commonly used in memory cards and USB flash drives for storage and transfer of data between computers and other digital products.

Folder: An area on a hard disk that contains a related set of files or alternatively, the icon that represents a directory or subdirectory.

Hard disk: A storage device that holds large amounts of data, usually in the range of hundreds to thousands of megabytes. Although usually internal to the computer, some types of hard disk devices are attached separately for use as supplemental disk space. "Hard disk" and "hard drive" often are used interchangeably but technically, hard drive refers to the mechanism that reads data from the disk.

Hardware: The physical components of a computer including the keyboard,

monitor, disk drive, and internal chips and wiring. Hardware is the counterpart of software.

Help desk: A help desk is an information and assistance resource that troubleshoots problems with computers or similar products. Corporations often provide help desk support their employees and to their customers via a toll-free number, website and/or e-mail.

Internet: A worldwide network based on the TCP/IP protocol that can connect almost any make or model of popular computers from micros to supercomputers.

IP address: Internet Protocol address; every computer connected to the Internet has a unique identifying number. Example: 192.168.100.2.

ISP: Internet Service Provider; an organization or company that provides Internet connectivity.

Knowledge base: A database where information common to a particular topic is stored online for easy reference; for example, a frequently-asked questions (FAQ) list may provide links to a knowledge base.

LAN: Local area network; a network that extends over a small area (usually within a square mile or less). Connects a group of computers for the purpose of sharing resources such as programs, documents, or printers. Shared files often are stored on a central file server.

Log in, log on: The process of entering your username and password to gain access to a particular computer; e.g., a mainframe, a network or secure server, or another system capable of resource sharing.

Malware: Software programs designed to damage or do other unwanted actions on a computer; common examples of malware include viruses, worms, Trojan horses, and spyware.

Network: A group of interconnected computers capable of exchanging information. A network can be as few as several personal computers on a LAN or as large as the Internet, a worldwide network of computers.

Password: A secret combination of characters used to access a secured resource such as a computer, a program, a directory, or a file; often used in conjunction with a username.

PC: Usually refers to an IBM PC or compatible, or when used generically, to a "personal computer". In a different context, PC also is an abbreviation for "politically correct."

PDA: Personal Digital Assistant; a small hand-held computer that in the most basic form, allows you to store names and addresses, prepare to-do lists, schedule appointments, keep track of projects, track expenditures, take notes, and do calculations

Program: A set of instructions that tells a computer how to perform a specific task.

Private cloud: Private cloud (also called internal cloud or corporate cloud) is a term for a proprietary computing architecture that provides hosted services to a limited number of users behind a secure and robust infrastructure.

Remote backup: A remote, online, or managed backup service is a service that provides users with a system for the backup and storage of computer files.

Remote desktop: A Windows feature that allows you to have access to a Windows session from another computer in a different location (XP and later).

Remote login: An interactive connection from your desktop computer over a network or telephone lines to a computer in another location (remote site).

Router: A device used for connecting two Local Area Networks (LANs); routers can filter packets and forward them according to a specified set of criteria.

Server: A computer that is responsible for responding to requests made by a client program (e.g., a web browser or an e-mail program) or computer. Also referred to as a "file server".

Software: Any program that performs a specific function. Examples: word processing, spreadsheet calculations, or electronic mail.

Trojan horse: A harmless-looking program designed to trick you into thinking it is something you want, but which performs harmful acts when it runs.

Tweet: An update of 140 characters or less published by a Twitter user meant to answer the question, "What are you doing?" which provides other users with information about you.

Twitter: A service that allows users to stay connected with each other by posting updates, or "tweets," using a computer or cell phone or by viewing updates posted by other users.

Upload: The process of transferring one or more files from your local computer to a remote computer. The opposite action is download.

USB: Universal Serial Bus; a connector on the back of almost any new computer that allows you to quickly and easily attach external devices such as mice, joysticks or

flight yokes, printers, scanners, modems, speakers, digital cameras or webcams, or external storage devices.

Username: A name used in conjunction with a password to gain access to a computer system or a network service.

Virtual classroom: An online environment where students can have access to learning tools any time. Interaction between the instructor and the class participants can be via e-mail, chat, discussion group, etc.

Virus: A program intended to alter data on a computer in an invisible fashion, usually for mischievous or destructive purposes. Viruses are often transferred across the Internet as well as by infected disks and can affect almost every type of computer. Special antivirus programs are used to detect and eliminate them.

VPN: Virtual Private Networking; a means of securely accessing resources on a network by connecting to a remote access server through the Internet or other network.

WAN: Wide Area Network; a group of networked computers covering a large geographical area (e.g., the Internet).

Wi-Fi: Wireless Fidelity; A generic term from the Wi-Fi Alliance that refers to of any type of 802.11 network (e.g., 802.11b, 802.11a, dual-band, etc.). Products approved as "Wi-Fi Certified" (a registered trademark) are certified as interoperable with each other for wireless communications.

WLAN: Wireless Local Area Network; the computers and devices that make up a wireless network.

Workstation: A graphical user interface (GUI) computer with computing power somewhere between a personal computer and a minicomputer. Workstations are useful for development and for applications that require a moderate amount of computing power and relatively high quality graphics capabilities.

World Wide Web: A hypertext-based system of servers on the Internet. Hypertext is data that contains one or more links to other data.

Worm: A program that makes copies of itself and can spread outside your operating system worms can damage computer data and security in much the same way as viruses.

ANNEX 1
LIST OF FC OFFICIAL SOFTWARE

NAME	BRIEF DESCRIPTION
HUMANIS	Human Resource Database of the Forestry Commission
WEB-BASED M&E	M&E Tool used in capturing and reporting on performance by all the Divisions of the Commission.
E-Document Management System	To facilitate the electronic storage and retrieval of incoming and outgoing correspondence, personal files, memos and letters
FLEETUS	Fleet Management System
ICT KLINIK	ICT Help Desk Management System
E-LIBRARY	To facilitate the electronic storage and retrieval of documents for the library
LEGDOCSYS	Legal Electronic Document Management System
FC CRUISE	Credit Union Management System
WTS	For tracking wood from the forest floor to mill and finally for export (ensuring legality of the source of wood)
MICROSOFT APPLICATIONS	For office use (Word, Excel, PowerPoint, etc)
WINDOWS OPERATING SYSTEMS	Servers = MS 2008, Version 2012 Desktop= XP, Win 7, 8 & 10
ESET SMART SECURITY	Corporate Anti-Virus
PFSENSE PROXY	Intrusion & Internet Bandwidth Monitoring
WIRESHARK	Network & Systems Monitoring Tool

SUN ACCOUNTS	Used for accounting purposes
REVCOMSYS	Revenue Collection and Management System for FC
PAYINFOSYS	Common Platform for sharing Centralized Payroll Information
FASYS	FC Availability System
CHARSYS	Charcoal Management Information System
FC-YEA CCMS	Call Centre Management System
YAMIS	Youth in Afforestation Management Information System
PVSYS	PV Tracking System for Internal Audit
STORMIS	Stores Inventory Management System
ESTASYS	Estate Management System
E-CONTRACT	Electronic management and payment system for contract staff
E-FORMS	Electronic form management system for FSD and TIDD Operations

ANNEX 2
EQUIPMENT DISPOSAL FORM

DEPARTMENT	
EQUIPMENT ITEMS	**ESTIMATED AGE** **ESTIMATED VALUE**
EQUIPMENT CONDITION Fully functional Partially functional Broken – known reasons Broken – unknown reasons	**DISPOSAL PLAN RECIPIENT** To be sold to---------- Donated (internally) to---------- Donated (externally) to---------- Donated (individual) to---------- Stripped and scrapped to----------
SIGNIFICANT HAZARDS	**MEASURES TAKEN TO ELIMINATE OR MINIMIZE RISKS**

The items referred to above have been inspected for potential risks to health and safety and the environment as far as reasonably practicable and have been assessed as fit to dispose.

Signed----------

Position----------

ANNEX 3
OFFENCES OF ICT USAGE

Offences of ICT usage can be categorized into three broad areas, namely; minor, major and intolerable.

MINOR

The minor offences are:

i. Failure to protect your desktop and or laptop computer from unauthorized access by External Agents or Commission's Staff.
ii. Failure to log off from applications, computers and networks when finished
iii. Leaving unattended personal computers with open sessions.
iv. Failure to secure your username and or password from other Users (authorized or unauthorized)

MAJOR

The major offences are as follows:

i. Failure of ICT Staff to ensure that security patches are applied to Users equipment.
ii. Any attempt by Users to access, copy, alter or delete the data of any other User without permission.
iii. Any attempt by Users to access networks or servers that the User has no legitimate reason to access, whether the User has the logical access rights to do so or not.
iv. Attempt by Users to pry into personal affairs of other Users without a legitimate purpose for accessing their data.
v. Disclosure of personal passwords to other Users without approval.
vi. Attempt by Users to repair /service ICT equipment without prior authorization from ICT Head or his/her Authorized Personal Representative
vii. Copying Forestry Commission's software for use on any computer other than Commission's supplied PC./that of the of FC.
viii. Copying or distributing FC's software to external parties without authorization from ICT Head.
ix. Engaging external consultants for software application development or buying off-theshelf software application without approval of the ICT Head or his/her Authorized Personal Representative.

x. Failure of ICT designated staff to ensure that the corporate anti-virus is updated as required.
xi. Disabling the anti-virus software or re-configuring any settings on the anti-virus software unless specifically authorized by the ICT Head or his/her authorized representatives.
xii. Disabling the firewall of the windows operating system unless specifically authorized by the ICT Head or his/her authorized representatives.
xiii. Failure to use officially assigned or allocated e-mail addresses in official correspondences within and outside the Commission.

INTOLERABLE

Intolerable offences are as follows:

i. Copying of FC's data for private use.
ii. Leaking out personal or confidential information relating to others or disclosing or otherwise revealing information of other Users without authorization.
iii. Transmission or otherwise dissemination of confidential materials by Users to third parties without prior authorization by ICT Head or his/her duly authorized representatives
iv. Creating and exchanging of messages that are offensive, harassing, obscene or threatening to other Users.

ANNEX 4
LIFESPAN OF ICT EQUIPMENT

No.	ICT Equipment	Primary lifespan	Secondary lifespan	Total No. of Years
1	Desktop Computers	4	2	6
2	Laptops/Notebook Computers	2	1	3
3	Handheld Computers	2	1	3
5	Server	5	2	7
5	Printers (Standalone)	3	2	5
6	Printers (Network)	5	3	8
7	UPS	2	1	3
8	Scanners	4	2	6
9	LCD Projectors	2	1	3
10	Switches	5	2	7
11	Routers (CISCO)	3	1	4
12	Routers (Others)	2	1	3
13	Firewalls	4	1	5
14	PABX	6	2	8
15	Voltage Stabilizer (3 Phase)	5	2	7
16	Voltage Stabilizer (Single Phase)	2	1	3
17	Core Network Infrastructure	8	4	12

ANNEX 5
DATA RETENTION FORM

RESPONSIBLE PARTIES **1. ..... 2. .....**	
DATA ITEMS	**RETENTION PERIOD**
FILE NAME ..... **LOCATION** ☐ In-house ☐ Off-site	**LEGAL REQUIREMENTS / SOURCE** .....

Originator: **Systems Administrator:**

Signed---------- Signed----------

Position---------- Position----------

Confirmed By: Head of ICT

Signed..... **Date:...../...../.....**

ANNEX 6
SOFTWARE REQUEST FORM

This form collects information to assist in the determination of the proposed software with the Commissions information and technology needs.

Please complete all fields, incomplete form needing more information will be returned.

Employee Name: _____ Department: _____

Location: _____

Software Description: _____

_____

_____

Is this request to replace existing software? ☐ Yes ☐ No

If yes, why is your current software inadequate?

_____

_____

_____

If no, explain your need for new software:

_____

_____

_____

Employee Signature: _____ Date: _____

For Official Use Only:

ICT Director Signature: _____ Date: _____

☐ Approved ☐ Not Approved

Reason:

_____

_____

_____