FC®

Forestry Commission

INFORMATION & COMMUNICATION TECHNOLOGY POLICY 2019

ABRIDGED VERSION

November 2020

TABLE OF CONTENTS

LIST OF ACRONYMS

ACRONYM	MEANING
FC	Forestry Commission
FCHQ	Forestry Commission Headquarters
FCTC	Forestry Commission Training Centre
FSD	Forest Services Division
ICSA	International Computer Security Association
ICT	Information and Communication Technology
ISP	Internet Service Provider
PDA	Personal Digital Assistant;
RMSC	Resource Management Support Centre
TIDD	Timber Industry Development Division
TNA	Training Needs Assessment
WD	Wildlife Division

SECTION ONE

1.1. INTRODUCTION

The introduction of corporate-wide use of ICT infrastructure has brought about a common platform for doing business effectively and efficiently. The increased efficiencies created from the use of Networks have also introduced new risks. The Forestry Commission has 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 FC and the liability imposed on them. Violations of this policy will be handled in accordance with the Terms and Conditions of the FC under which offences are classified as Minor, Major and Intolerable (Refer to Appendix 3 in the main document). For further details of any item in this Abridged version, kindly refer to the full version of the Policy.

1.2. Purpose

Users of ICT resources of FC must adhere to strict guidelines concerning the appropriate use of these resources 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 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.

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 taff.

vii. Provide guidelines for the proper acquisition and disposal of computer equipment

SECTION TWO

2.1.1. 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, fingerprints 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 default/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.

2.1.2. 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.

2.1.3. Remote Access

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.

2.1.4. 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.

2.1.5. AUTHORIZED USE AND PRIVACY

2.1.5.1. 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.

2.1.5.2. 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

Users must report all ICT related requests for service to the ICT department and Zonal
Offices.

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.

2.3.1. Antivirus Protection

- FC Approved antivirus must be installed on all the computers on the Commission Network.
- The Commission should ensure that original licensed versions of software are procured to ensure update of patches.

2.3.2. Corporate And Bundled Centralised Antivirus

Antivirus software preinstalled on new computers will be replaced with corporate versions of antivirus software in use by the Commission.

2.3.3. Updates

- Antivirus software must be automatically updated daily since new viruses appear very regularly.
-

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 Help desk 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 reconfigure 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

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. 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 serverspecific 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.

3.1.2. 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** first name + 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.

3.3. 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. 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.

4.1.2. 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 re-employed 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. 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.

5.1.2. 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.

5.1.3. 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.

5.1.4. Exemptions And Waivers

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

5.1.5. 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.

5.1.6. 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.

5.1.7. 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.

5.1.8. 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. 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.

6.1.2. Data Management

The Commission shall utilize Data management tools and techniques to manage the Data Architecture, Formats, Usage, Access, Control, Management, Backup and Retention

6.1.3 Data Backup

i. It is mandatory for users to store important files on FC's backup Mediums and comply to ICT backup directives concerning official data storage on their client equipment (computers, laptops, handheld devices, ipads etc).

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.

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

- SECURITY ACCESS CONTROL (SECURITY)
- DUAL MODE OF OPERATION (ONLINE AND OFFLINE)
- PROTECTION OR COPYRIGHTING OF SOURCE CODES

SECTION SEVEN

7.1. ICT TRAINING

7.1.1. 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

7.1.2. 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.

7.1.2.1. 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)

7.1.2.2. Training Resources

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

7.1.3. Training Methods

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

7.1.3.1. Formal Classroom Training

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

7.1.3.2. 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. 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;

8.1.2. 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.

8.1.3. 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.