INFORMATION AND COMMUNICATIONS TECHNOLOGY POLICY

OCTOBER 2017

NCDC
NATIONAL CURRICULUM DEVELOPMENT CENTRE

INFORMATION AND COMMUNICATIONS TECHNOLOGY POLICY

OCTOBER 2017

NCDC

NATIONAL CURRICULUM DEVELOPMENT CENTRE

Published by:

National Curriculum Development Centre ,
P.O. Box 7002,
Kampala.

ISBN: 978-9970-00-194-1

www.ncdc.go.ug

Designed by Dickson Amanya

CONTENTS

FOREWORD

The achievement of information systems security and knowledge at NCDC is one of the main priority areas towards the attainment of the strategic goals and objectives in curriculum development and Uganda's National Development Goals enshrined in Vision 2040.

The NCDC ICT Policy is inspired by the need to align the use of ICTs as an enabler in curriculum design, development and teaching to transform NCDC into a leading curriculum development hub in the region.

In developing this policy, NCDC has taken into consideration the tremendous impact of ICT in teaching and learning visa-viz traditional approaches to teaching and learning. Each section of the policy has a background and guidance to the Dos and Don'ts s of the policy.

Emphasis will be placed on the use of this policy as a control measure to safeguard the usage of ICTs at NCDC in line with other national and international ICT policies and regulations.

Dr Elizabeth Ezati
Chairperson
Governing Council

ACKNOWLEDGEMENT

NCDC would like to thank everyone who worked tremendously towards the production of the ICT Policy as a control tool to the usage and access of ICT systems at the Centre.

We would like to thank the ICT team, and all those who worked behind the scenes for their professional input.

Special thanks go to NCDC Management for supporting the work.

Last but not least, NCDC would like to thank Academic Steering Board and Governing Council for having accepted and approved this policy as a control and guiding tool for ICT usage at NCDC.

Let this policy be implemented for the good of the Centre.

Grace K. Baguma
Director
National Curriculum Development Centre

ACRONYMS AND ABBREVIATIONS

BYOD	Bring Your Own Device
CAT	Category
CD	Compact Disc
DHCP	Dynamic Host Configuration Protocol
ICT	Information and Communications Technology
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISO	International Organisation for Standardisation
ISP	Internet Service Provider
ITU	International Telecommunications Union
LAN	Local Area Network
MDAs	Ministries, Departments and Agencies
MDF	Main Distribution Facility
MoES	Ministry of Education and Sports
NCDC	National Curriculum Development Centre
NITA	National Information Technology Authority
PBX	Private Branch Exchange
PODs	Personally Owned Devices
RDBMS	Relational Database Management Systems
ROM	Read only Memory
SLAs	Service Level Agreements
SSID	Service Set Identifier
TCP/IP	Transmission Control Protocol/ Internet Protocol
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WAP	Wi-Fi Access Point (WAP)

DISCLAIMER

This document MUST be used in consultation with the general ICT guidelines developed by NITA-U, NCDC Standing Orders, and any other legal document that governs the activities of the National Curriculum Development Centre as a Government Institution.

1.0 INTRODUCTION

Information and Communications Technology (ICT) has become the backbone of day-to-day operations in all organisations in the 21st Century. National Curriculum Development Centre (NCDC) has not been an exception. In recognition of ICT as an enabler to the attainment of organisational goals, NCDC developed this ICT Policy to streamline ICT utilization, deployment and investment as well as manage its relationships with its internal and external customers.

While Council and Management of NCDC recognise this fact, organisations the world over, including NCDC, are faced with the challenges of ICT security and establishment of acceptable use of ICTs as well as legal compliance. This ICT Policy therefore seeks to provide guidelines for acceptable and secure use of ICT by both NCDC employees and business partners. The contents of the ICT Policy must, however, comply with other NCDC guidelines, as well as the national laws.

This ICT Policy comprises a number of sections covering the aspects of Hardware, Software, Infrastructure, Management Information Systems, Security and Access Control, Communication, Business Continuity and Procedures.

1.1 About NCDC

NCDC's Vision

A holistic Curriculum for producing responsible Citizens equipped with productive skills.

Mission

To develop curricula and instructional materials for equitable and quality education through research, innovation and stakeholder involvement

Core Values

Teamwork, Integrity, Equity and Excellence (TIEE)

Mandate

The Centre is a corporate autonomous body of the Ministry of Education and Sports (MoES). It is responsible for inter-alia development of curricula and related materials for various levels of education i.e. Pre-Primary, Primary, Secondary and Tertiary, organising capacity building courses for stakeholders on curricula and matters related to curriculum.

1.2 Functions of NCDC

a) To investigate and evaluate the need for syllabus revision and curriculum reform at Primary, Secondary and Tertiary levels of education in pre-school and post-school education and teacher education.
b) To initiate new syllabuses, revise existing ones, carryout curriculum reform, research, testing and evaluation, update and improve syllabuses for school and college courses.
c) To draft teaching schemes, textbooks, teacher's manuals and examination syllabuses in cooperation with teaching institutions and examining bodies.
d) To design and develop teaching aids and instructional materials.
e) To devise, test and evaluate examination questions and methods of examining students with other appropriate teaching and examining bodies.
f) To organise and conduct in-service courses of instruction for the acquisition of knowledge and professional skill by persons intending or required to teach new courses developed at the Centre.
g) To organize and conduct courses in the objectives and methods of curriculum development for persons required to participate in curriculum development work.
h) To hold seminars and conferences on curriculum development projects and problems.
i) To collect, compile and analyse abstract statistical information on curriculum and matters related to curriculum.
j) To publish information, bulletins, digests, periodicals or other written material concerning curriculum and other matters related to curriculum.
k) To disseminate and promote general and better knowledge and understanding of new curricula, teaching methods and teaching aids.

1.3 NCDC ICT Mission

To effectively utilise ICT as a tool for effective management of curriculum development, dissemination and evaluation processes.

1.4 Objectives of the Policy

The objectives of this ICT Policy and procedures are to ensure that:

a) information is created, used and maintained securely.

b) all NCDC's computing facilities, programs, data, networks and equipment are adequately protected against damage, loss, misuse or abuse.

c) appropriate security measures are employed as part of the effective implementation of ICTs in NCDC.

d) all users understand their own responsibilities for protecting the confidentiality and integrity of the data and information they handle.

e) all NCDC ICT assets can be identified.

f) asset and business risks associated are minimised.

g) NCDC information systems are effectively and efficiently used by NCDC employees and affiliates.

h) ICT systems are available and functioning.

i) there is awareness that appropriate information and physical security measures are implemented as part of the effective operation and support of ICT facilities and services

j) all users fully comply with Information Security Policy, standards, guidelines and procedures, and the relevant NCDC legislation.

1.5 Benefits of the Policy

The Policy provides and encourages good practices in the acquisition, deployment, usage and management of ICT resources in order to:

1. synchronise the deployment and usage of ICT resources at the Centre.
2. reduce duplication and overlap of technology, data and procedures.
3. support asset compilation, validation and valuation.
4. enhance directed ICT investment at the Centre, inter-operability, portability and security.
5. reduce the total cost of equipment acquisition through sharing of common facilities.
6. increase opportunities for partnering and exploring new technologies.

1.6 Scope of the Policy

Achieving NCDC's overall strategic objectives is dependent on efficient usage and management of its resources and information/data. This ICT Policy covers the following aspects:

1. **Bring Your Own Device (BYOD) Covering**: Description and Guidelines of using employee's own devices to accomplish employer's tasks
2. **ICT Hardware Covering**: Procurement and deployment of ICT Hardware; ICT hardware maintenance; Hardware warranty; Hardware requisitioning; Hardware disposal; Hardware transfer; and Documentation;
3. **Software Covering**: Software purchases and deployment; Licensing; Upgrades and Documentation;
4. **Information Systems and Office Automation Covering**: Development/ Deployment of new Information Systems; Training; Documentation; Upgrades and patches; Use of standard indicators; Post-installation support; Choice of

database software; Data sharing; Data backup; Systems architecture; and Data collection support

5. **ICT Infrastructure Covering**: Local Area Networks (LANs); Wide Area Networks (WANs); Network Backbone; Network Operations Centre; Power Supplies and Cabling and Physical Access Controls
6. **Telecommunications Services and the Internet Covering**: Deployment of telephone services; Provision of Internet; Use of Internet; Use of e-mail; Naming of e-mail addresses; Backup of e-mails; Design and maintenance of NCDC website
7. **Security Covering**: Use of user accounts; Domains; Password ageing; Password standards policy; Password security; Access to ICT equipment rooms; Transferring equipment offsite; Disposal of equipment; Reporting of security incidents; Change Control; Encryption
8. **Network Access Covering**: Network access policy; Server connectivity; Connectivity of privately owned equipment; Access controls; Wireless access network points; E-government; Network administration; Conditions for use of NCDC network
9. **Anti-virus and Spam Covering**: Procurement of anti-virus software; Installation of anti-virus and updates; Administration responsibilities; Anti-virus implementation policy guidelines
10. **Database backup and Disaster Recovery**: Data backup; Responsibility for data backup; Desktop backups; Best practice backup procedures; Disaster recovery; Best practice for disaster recovery procedures

1.7 ICT Policy Development Process and Implementation

The Policy has been developed through a consultative process which has seen all Departments and Units, existing legal framework and NCDC management consulted.

Two approaches were used in the development of this policy:
First, interviews were held with NCDC senior management and employees to obtain an in-depth assessment of ICT situation in NCDC, desired future direction and gaps. Through the same interviews, the ICT Unit obtained departmental strategic plans, established how they utilise ICTs for business and how they would like to utilise ICTs in the immediate and distant future to improve efficiency and effectiveness in service delivery. Involving NCDC staff and other stakeholders in policy formulation process does not only serve to provide information, but also increases ownership and guarantees smooth implementation;
Secondly, secondary data/documents were reviewed. These included the National IT Policy, the e-Government Policy Framework, Ministry of Education, and Sports ICT Policy, the ICT Policy Implementation Framework for Local Government 2009 and NCDC-FMIS Requirements Analysis Report (2012).

It was a result of the above approaches that a draft ICT Policy was produced. This draft was then reviewed by the ICT Unit, staff and senior management and based on their feedback, the final ICT Policy produced. The final ICT Policy was then submitted to the NCDC Governing Council for approval.

1.7.1 Legal Framework

All NCDC's ICT facilities and information resources remain the property of NCDC and not of particular individuals, teams or departments.
This Policy conforms to the NCDC mandate as stipulated in the NCDC Act - Cap. 135 Laws of Uganda, the National IT Policy 2010, the Government of Uganda e-Government Policy Framework 2010, Ministry of Education and Sports ICT Policy 2006, Ministry of Information and Communication Technology ICT Policy and the ICT Policy Implementation Framework for Local Government 2009

The Policy is also compliant with World Technology Standards such as: ISO, IEEE and International Telecommunications Union (ITU);
Guidelines for Operation, Usage and Management of Information Technology Infrastructure in government Ministries, Departments and Agencies (MDAs) & Local Government; The Computer Misuse ACT, 2011; Guidelines and Standards for Acquisition of IT Hardware & Software for MDAs; Standards for Structured Cabling for Government MDAs; E-Government Regulations 2014; Guidelines for Development and Management of Government Websites; Standards for Structured Cabling for Government, Ministries, Departments and Agencies 2014 or later.

1.7.2 Non-Compliance

Any breach of this Policy or associated ICT Policy will be managed in accordance with the Disciplinary measures as contained in relevant NCDC statutes and/or employer-staff agreements.

1.7.3 Responsibilities

The ICT Committee (*See Appendix II*) on behalf of NCDC Management oversees the overall implementation of this policy. All reviews and amendments to this policy document must be taken through the ICT Committee, forwarded to Management for consideration and onward submission to the NCDC Governing Council for approval.

ICT committee must undertake regular risk reviews to ensure that all risks are identified and all reasonable measures taken to prevent security breaches. The Systems Administrator is mandated to maintain the security and integrity of NCDC's ICT Infrastructure, facilities and services.

2.0 GUIDELINES

2.1 Bring Your Own Device Guidelines

Bring Your Own Device (BYOD) describes a situation where employees bring Personally Owned Devices (PODs) (laptops, tablets, and smart phones, etc) to their workplace, and use them to access privileged company information and applications as they do company work. This is currently applies to the situation at NCDC.

There are some key advantages to operating a BYOD strategy, the major one being cost savings (reduced hardware expenses, software licensing and device maintenance) on the side of NCDC. While BYOD sounds attractive, we need to consider the full implications of allowing corporate data to be accessed on personal devices over which the Centre has little or no control. Increased use of ICT services at NCDC with PODs can bring with it an increased risk from threats such as hackers and viruses. "**This is where convenience clashes with security**". It is therefore advisable that if funds allow, all NCDC staff be given ICT devices to aid their work.

There might also be cost implications. Even though ICT hardware expenses can potentially be reduced with a BYOD approach, it may cost more for a company to integrate and support a diverse range of employee devices.

The following guidelines will be applicable to persons under the BYOD arrangement;

i) All users are requested to register their devices with the Systems Administrator.
ii) Since NCDC does not have the resources or expertise to support all possible devices and software, PODs under BYOD arrangement will receive limited support on a 'best endeavours' basis for NCDC's business purposes only. This support shall be in terms of Software installation and updates, Antivirus installations and updates, Repairs and Maintenance and network access configuration only for the item(s) registered above.
iii) It is the user's responsibility to ensure security and safety of NCDC data on his device at all times by password protecting the device.
iv) User accepts to delete all NCDC data from his/her device at his/her time of exiting NCDC employment.
v) Individual users of PODs must ensure that valuable corporate data created or modified on PODs are backed up regularly, preferably by connecting to the corporate network and synchronising the data between POD and a network drive, otherwise on removable media stored securely.
vi) The user is obliged to take care not to use POD to infringe other people's privacy rights while at work like making audio-visual recordings at work on your POD.

2.2 ICT Hardware Guidelines

This section presents guidelines that govern the procurement, disposal, deployment, usage and investments in ICT hardware.
Information and Communications Technology Hardware is an umbrella term that includes any communication device or application encompassing: radio, television, cellular phones, computer and network hardware and software, satellite systems, etc as well as various services and applications associated with them such as video conferencing and distance learning.

2.2.1 Scope

This Policy covers:

a) Procurement and deployment of ICT Hardware
b) Hardware maintenance
c) Hardware Disposal
d) Hardware requisitioning
e) Identification of ICT Hardware
f) Registration of ICT Assets
g) ICT Hardware Storage

2.2.2 Procurement and Deployment of ICT Hardware

a) It is NCDC's policy to procure genuine ICT hardware from authorized resellers or dealers or agents based on specifications provided by user departments and approved by the ICT Committee following the National Information Technology Authority (NITA) guidelines. Such specifications shall be shared by the ICT Committee regularly (through e-mails or any other information sharing mechanisms) and shall be updated as need arises

b) It is NCDC Policy that for all ICT hardware procured or received as donations to comply with the minimum warranty periods shown in the table below (Refer to NITA specifications: www.nita.go.ug). These warranty periods exclude equipment failure caused by power fluctuations.

No	Equipment type	Minimum Warranty Period (years)
1	Desktop computers (Hardware)	1
2	Laptops, Notebooks, Tablets or other portal devices	1
3	Servers	2
4	Switches, routers, hubs, patch panels, modems	1
5	Telephones (Desk sets, handhelds, mobiles, etc), Faxes	1
6	Printers	1
7	Scanners	1
8	Projectors	1

No	Equipment type	Minimum Warranty Period (years)
9	Uninterrupted Power Supplies (UPS)	2
10	Television	1
11	CCTV	1
12	Flash Disks	1
13	Equipment racks	1
14	Personal Digital Assistants (PDA), Smart phones	1

c) All hardware purchased or deployed at NCDC shall be accompanied by manufacturer installation and other administrators' manuals (whether in soft or hardcopy);

d) It is a policy to securely store hardware documentation by the Head of IT or any designate for future reference.

2.2.3 Hardware Maintenance

a) It is a policy to enter into Service Level Agreements (SLAs) with ICT service providers for hardware maintenance (for periods of at least one year) and to ensure such agreements comply with PPDA procurement guidelines. The SLAs must explicitly list the tasks to be performed by the service provider, key performance indicators, response times, penalties for non-compliance, NCDC roles, pre-liquisites for operationalisation of the SLAs, conflict resolution procedures and agreed upon arbitration authority to be referred to in case of a conflict.

b) It is a policy that the service provider engaged in maintenance of NCDC hardware shall work under the supervision of the Systems Administrator or his designate and that the service provider shall be governed by confidentiality and other applicable laws of NCDC and government of Uganda.

c) It is a policy to report any ICT hardware or software malfunctions to the ICT Unit by filling the ICT Fault Report Form (See copy in appendix 1). If the external assistance is deemed necessary, such support shall be arranged by the ICT Committee.

d) It is a policy to log all hardware maintenance activity in an up-to-date register, showing nature of the problem encountered and solution used to address the problem.

2.2.4 Hardware Disposal

a) All ICT hardware that is due for disposal (subject to NCDC hardware disposal guidelines such as age, condition, and so on), shall be cleaned of all data/ information prior to submission to Procurement and Disposal Unit for eventual

disposal.

b) ICT hardware shall be disposed in line with PPDA guidelines, NITA and other relevant international laws.

c) All ICT hardware register shall be updated by the Systems Administrator to mark each of the items disposed as 'DISPOSED'.

d) All temporary electronic storage items (e.g floppy disks, CD's) should be over-written wherever possible with randomly generated characters using software designed for this purpose and reformatted prior to disposal. If an electronic storage item cannot be overwritten, it should be physically destroyed and/or burnt.

e) Disposal of ICT equipment shall be done in line with the current government environmental laws and other international laws.

2.2.5 Identification of ICT Hardware

It's a policy to engrave ICT hardware with unique numbers that are to be generated by the ICT Unit. Codes shall be based on ICT categories such as Computers, Printers, Power backups, Fax machines, etc.

2.2.6 Asset Registration

It's a policy to maintain an up-to-date ICT equipment asset register comprising of asset serial and engraved numbers, make, type, model, year of purchase, cost of asset, specifications (where applicable) and location. This register shall be managed by the Systems Administrator.

No	Asset Name	Brand	Serial No	Engraved No	Year of acquisition	Cost(UGX)	Specifications	Location	Remarks

2.2.7 ICT Hardware Storage

a) It is a policy to have all ICT assets covered with dust-free clothes as a safety precaution;

b) Its NCDC policy to have server rooms and ICT resource centres designed to meet the minimum standards, i.e lockable doors, burglar proof and air conditioned;

c) It is NCDC policy in situations where there is no built server rooms, server racks shall be implemented to secure the servers;

d) It is NCDC policy that each ICT equipment user will be responsible for ensuring that whenever ICT hardware equipment relevant to his/her particular system is located, the surrounding environment is fully conducive to the ICT equipment's operational tolerances. This will necessitate the monitoring of temperature, humidity, power supply quality, etc prior to the installation or sitting of the ICT hardware equipment;

e) Its NCDC policy that each system user must ensure that no item of ICT hardware equipment be cited in any location where there exists the potential threat of water damage or any other natural disaster;
f) All personnel should be actively discouraged from smoking, eating and/ or drinking in rooms, areas or departments where ICT hardware equipment is located; NCDC policy that in case of fire, all rooms, areas or departments housing ICT hardware equipment should have ready access to fire fighting equipment as well as appropriate fire detection and prevention systems. However, special notice should be given to the location of water sprinkler units.
g) It is NCDC policy that any movement, relocation, assignment of ICT equipment or peripheral to an office shall require approval from the Systems Administrator and proper documentation.

2.3 Software Guidelines

Software is defined as any application, operating system, database or other ICT system used to collect process or store data in an electronic format. Software is used to process, manipulate and store data at NCDC. It is essential that all software meet minimum standards to the integrity and safety of NCDC's information. This section gives advice on how Software guidelines will be implemented.

2.3.1 Scope

This section covers:

a) Software purchases and deployment
b) Licensing
c) Upgrades
d) Installation of Software
e) Recommended practices and Implementation procedures

2.3.1 Purchasing Software

Software to be deployed or procured for NCDC shall:

a) be purchased from authorised resellers of a renowned manufacturer.
b) include warranty of at least one year within which period NCDC shall be entitled to upgrades and acquisition of patches for bug fixing at no extra cost.
c) have the physical and postal addresses of the vendors maintained for ease of future communication.

2.3.2 Software Licensing

a) All software installed in NCDC shall bear genuine manufacturer's license valid for the period agreed upon during acquisition.

b) NCDC shall maintain a register of licenses held managed by the Systems Administrator. Key attributes for documentation shall include software name, license keys and validity period. This register shall be used to claim for licenses where hardware on which it is installed is damaged and NCDC is unable to trace the original installation media.
c) At no time whatsoever shall NCDC share software licenses with unauthorized people/organisations as this is likely to attract Law suites of the offenders.

2.3.3 Software Upgrades

NCDC or other software providers shall ensure that the software installed in NCDC is kept up-to-date. This requirement shall be included in the agreements signed with the vendors at the time of purchase.

2.3.4 Installation of Software on NCDC Computers

a) Only genuine and authorized software shall be installed on NCDC systems with the approval of the ICT Committee.
b) Software or applications that are not of interest to the business of NCDC but may adversely affect the bandwidth, e.g. audio files and others in the same category, shall not be installed and activated on the NCDC computer systems. Downloading of data files and software from other networks or on any other medium must be controlled to ensure proper utilisation of the ICT resources.
c) Regular reviews of the software and data content of systems supporting critical business processes should be conducted and the presence of any unapproved files or unauthorised amendments should be formally investigated.

2.3.5 Software Documentation

a) All software purchased or deployed in NCDC shall be accompanied by manufacturer installation and other administrators' manuals.
b) Such manuals may be in hard or soft copy depending on NCDC's specifications at the time of purchase.

2.4 Information Systems and Office Automation Guidelines

An information system may be defined as a combination of databases, human and technical resources that together with appropriate organisation skills can produce information needed to support a certain economic activity, management of resources and/or decision-making procedures.

2.4.1 Scope

This section covers:

a) Development of new information systems
b) Deployment of new information systems
c) User training on new information systems
d) Documentation
e) Upgrades and patches
f) Use of standard indicators
g) Post installation support
h) Choice of database software
i) Data sharing
j) Systems architecture

2.4.2 Development and Deployment of new Information Systems

Due to the nature of work, NCDC encourages in-house software/application development to increase the efficiency of automation, and also enable NCDC to reduce costs on software maintenance as local personnel improve their skills in system development.

a) All staff or vendors intending to develop new information systems for use in NCDC shall do so in consultation with the head of ICT Unit or his/her designate and the intended system users prior to commencement. The approval shall be obtained from Management.
b) The need for such services should be formally approved by the line manager, and formally communicated to the ICT Committee.
c) Care MUST be taken during development not to disrupt the operations of NCDC IT systems.
d) All ICT innovations developed by NCDC staff during their term of office while using NCDC's resources by default are properties of NCDC. For those developed by partners using NCDC infrastructure, NCDC may claim benefits depending on the nature of agreement signed.
e) New information systems shall be built on the existing systems thereby enriching the existing systems with additional features, in addition to decongesting NCDC ICT infrastructure with lots of information systems. This will also eliminate duplication of efforts.
f) The naming (nomenclature) to be used in developing new systems shall conform to the existing NCDC standards to ease support and maintenance. Such a nomenclature shall be prepared by the Head of ICT Unit with support from the Software Development and Support section and shall be revised from time to time, to keep it in line with developments worldwide.
g) There shall always be a clear contract between the system supplier and the representative of NCDC clearly stipulating the issues that must be accomplished

prior to the deployment of the new software (e.g. expected documentation, deployment schedule, training and type of staff expected to be trained).

2.4.2.1Recommended Practices and Implementation Procedures

The design and implementation of the information system supporting the business process can be crucial in terms of service delivery and security. Therefore user requirements MUST be identified and agreed upon by the user department and the developer prior to the development and/or implementation of the system.

2.4.2.2 Requirements Analysis and Specifications

a) The developer MUST state business requirements for new information systems, or enhancements to the existing information.
b) Specifications for the requirements for controls MUST consider the automated controls to be incorporated in the information system, and the need for supporting manual controls.
c) Similar considerations MUST be applied when evaluating software packages, developed or purchased for business applications.
d) Requirements and controls MUST reflect the business value of the information assets involved and the potential business damage which might result from a failure or absence of security.
e) System requirements for information security and processes for implementing security MUST be integrated in the early stages of information system development. Controls introduced at the design stage are significantly cheaper to implement and maintain than those included during or after implementation.

2.4.2.3 Correct Processing in Applications

a) Appropriate controls MUST be designed into applications to ensure correct processing. Such controls include: the validation of input data, internal processing and output data.
b) Additional controls may be required for systems that process or have an impact on sensitive, valuable or critical information. Such controls MUST be determined on the basis of security requirements and risk assessment.

2.4.2.4 Input Data Validation

a) Data input to applications must be validated to ensure that this data is correct and appropriate.
b) Checks must be applied to the input of business transactions, standing data (such as names and addresses and parameter tables)

2.4.3 Upgrades and Patches

Suppliers of information systems to NCDC shall, from time to time, provide updates of the said systems to fix any identified bugs in the software.

2.4.4 Choice of Database Software

a) All information systems developed for NCDC shall be developed using Relational Database Management Systems (RDBMS) to ease sharing of information with other sectors/stakeholders/users and linkage to existing systems.
b) All new software providers shall among other things, consider use of already existing RDBMS to maximise utility and avoid unnecessary costs through duplication.
c) New systems developed for NCDC shall be thoroughly tested prior to rollout.

2.4.5 Post Installation Support

As one of the requirements, the providers of new information systems at NCDC shall be required to provide post-installation support to NCDC for as long as it is required to run the application at NCDC. The time span of this support shall be indicated in the respective contracts.

2.4.6 Data Sharing

To facilitate sharing of data to and from other systems within or outside the NCDC systems, all new information systems developed shall posses import/export features.

2.4.7 Training

a) Any entity or individuals that develop(s) for and deploy(s) software at NCDC shall accompany it with satisfactory training to the end-users, systems administration staff and management staff to enable effective implementation of the new system.
b) The staff of the ICT Unit shall be trained to provide first level support, troubleshooting and resolution and/or maintenance.
c) New systems should be accompanied by a user manual for day- to- day reference by the NCDC users.

2.4.8 System Architecture

Information systems to be deployed in NCDC shall be developed to run on multi-user environments (web-based) for ease of deployment and maintenance.

2.5 ICT Infrastructure Guidelines

Information and Communications Technology (ICT) infrastructure refers to Local and Wide Area Networks (LANs and WANs), network backbone, telephone networks, power supplies and related cabling, data centres/ server rooms.
This ICT infrastructure policy therefore defines guidelines for usage and deployment of these technologies in NCDC.

2.5.1 Scope

ICT Infrastructure covers:

i). Local Area Networks
ii). Wide Area Networks
iii). Wireless Networks
iv). Network Backbone
v). Network Operations Centre
vi). Power Supplies and Cabling
vii). Data Centre/Server Room

2.5.2 Local Area Network

A Local Area Network (LAN) may be defined as a collection of autonomous computers and other related devices that are interconnected so as to share resources within a small geographical area. The shared resources may be documents, computer systems, hardware and reports.

2.5.2.1 Adding and Connecting Equipment to the LAN

While connecting to NCDCs network, all network users shall comply with the following policy statements:

a) All equipment connected to NCDC's network shall conform to the appropriate standards as set periodically by the ICT Committee and run only across the backbone of those protocols supported by NCDC.
b) Only authorised staff shall add ICT equipment to the NCDC network.
c) All equipment connecting to NCDC LAN shall go through a central server.
d) All systems to be connected to NCDC LAN must comply to NCDC's Systems Health check (must have an updated antivirus, active firewall, updated windows and patches, malware and spyware software etc)

2.5.2.3 LAN Acceptable Use

It is NCDC policy that authorised users may access the Internet for NCDC business or

personal information provided that they:

a) do not jeopardise the security of any NCDC information which may be present on the computer being used to access Internet.
b) do not violet any of the NCDC's policies.
c) do not engage in illegal activities.
d) do not engage in outside business interests.

2.5.2.4 Server Connectivity

The connection and use of a computer server shall be authorised by the ICT Committee. All servers shall be handled by the systems administrator who is responsible for:

a) Server administration and maintenance.
b) Server security including but not limited to data backup, access control, operating system and application updates and security patches.
c) NCDC reserves the right to bar access to information servers containing material considered illegal or likely to bring the respective NCDC offices into disrepute.
d) NCDC shall not be liable for any loss or damage suffered by the information owner as a result of barring access to or removal of material and information that is stored on individual machines. Users are advised to store information on the available network drives.

In the event that a connected user is causing an unacceptable level of interference with the operation of the NCDC network, the Systems Administrator, with justification, shall take action to disconnect the user from the network.

2.5.2.5 Connectivity of Privately Owned Equipment

Staff and panel members may connect computing equipment to the NCDC network only with the permission of the ICT Unit. Such equipment or systems shall be subjected to NCDC rules/regulations/policies currently in force. Such conditions shall include pre-scanning of these devices to ensure they are clean prior to use on NCDC network. Other conditions shall include obtaining express permission from NCDC Head of ICT Unit or Systems Administrator or his designate before use especially in areas where they are prohibited.

2.5.2.6 Network Administration

a) All network addresses including IP addresses, shall be allocated and administered by the Systems Administrator.
b) Requests for extra cabling or the insertion of wireless networking devices within a department/building shall be addressed to the Systems Administrator and authorised by the ICT Committee.
c) The Systems Administrator in consultation with the ICT Committee shall regulate

use of the backbone bandwidth. In the event of unacceptable events occurring on the network, the Systems Administrator in consultation with the users shall identify the cause and if need be request the immediate removal of any devices or equipment believed to be the source of the problem from the network.

d) In the event of some parts of a network causing problems on another part of the NCDC network or on an external network, the Systems Administrator shall have the right to disable any part of the network as necessary in order to remove the source of the problem.

2.5.2.7 Conditions for use of NCDC Network Facilities

All users of the NCDC network and attached devices shall comply with the security policies and all other conditions for use as spelt in this ICT Policy and related documents. Breaking any of the underlying conditions shall lead to disciplinary procedures being invoked with penalties which could include suspension from the use of all NCDC ICT facilities for extended periods. Serious cases shall be referred to management for action.

2.5.2.8 Network Structure

It is NCDC policy that the basic structure of the computer network at NCDC will be a client/server domain controller on a fast Ethernet network running TCP/IP. The primary network at NCDC will be based on an extended star topology.

2.5.2.9 Physical Structure/ Layers 1-2

The primary media used for vertical drops will be CAT 6 (or higher cable) with RJ45 or keystone Jacks for terminations. Patch panels and keystone jacks will be wired using the T568B standard. 802.11(x) will be used for wireless networking when and where appropriate.

Horizontal runs between the Main Distribution Facility (MDF) and the Primary Intermediate Facilities (PIF) locations will utilise fibre optic cable within a minimum rating 1 gigabit. Horizontal runs from a primary PIF to a local switch will utilise CAT6 of higher cable. All switches will be rated at 100 megabit or higher, with new acquisitions being VLAN capable.

The Systems Administrator will from time to time give guidance on network physical structure in consultation with NITA general guidelines.

2.5.2.10 Protocols

NCDC's computer network will use TCP/IP as the primary protocol. TCP/IP addresses

will be assigned to servers, network appliances (switches, etc), network printers and other devices designated by the Systems Administrator. The TCP/IP addresses used will be one of the private sets reserved for private networks. The Systems Administrator will assign internal addresses utilising the following scheme:

i). Servers and Network Devices: 192.168.2.xxx
ii). IP Telephony Devices: 192.168.2-4.xxx
iii). Workstations: 182.168.5-10.xxx (generally set by DHCP)

The Systems Administrator will assign all public TCP/IP addresses to the appropriate devices (such as the Web and E-mail servers) using those numbers assigned to NCDC by the Internet Service Provider (ISP).

2.5.2.11 Wireless Networks

The Systems Administrator shall be responsible for providing a secure and reliable NCDC wireless network. Under this broad responsibility, the following NCDC wireless guidelines shall apply:

a) Only hardware and software consistent with wireless standards approved by the ICT Committee shall be used for wireless access points.
b) In the event that a wireless device interferes with other equipment, the Systems Administrator shall resolve the interference.
c) Deployment and management of wireless access points in strategic areas at NCDC shall be a responsibility of the Systems Administrator.
d) All users of wireless access points shall be given access rights by the Systems Administrator.

3.0 TELECOMMUNICATIONS SERVICES AND INTERNET GUIDELINES

Telecommunication is the exchange of information using electronic media. Today, telecommunication is widespread and devices that assist the process such as the telephone, computers, radio and television are common in many parts of the world. There is also a vast array of networks that connect these devices; including computer networks, public telephone networks, radio networks and television networks.

This policy, therefore, covers all issues associated with use of computer infrastructure for communication both within and outside NCDC.

3.1 Scope

a) Deployment of telephone services
b) Provision of Internet
c) Use of Internet
d) Use of electronic mail (e-mail)
e) Naming of e-mail addresses
f) Backup of e-mails
g) E-Government
h) Design, development and update of websites of NCDC.

3.2 Deployment of Telephone Services

NCDC shall install Private Branch exchange (PBX) or other appropriate technologies when installing telephone systems. The PBX shall consist mainly of several branches of telephone systems to switch connections to and from connections. It shall be used to connect all internal phones to an external line. Connected this way, NCDC shall lease one or more lines and have many people using it, with each one having an extension at their desk.

3.3 Internet

NCDC is committed to the use of the Internet to support its staff in achieving operational efficiency. Internet policies are therefore supposed to ensure that Internet is used for good causes and is not abused. It is NCDC policy to ensure that suitable controls are in place to prevent security breaches or other negative consequences not forgetting that networks used for the Internet are not secure and any communication sent by this means could be accessed or modified by unauthorised individuals. There are also threats from obtaining information from the Internet with virus attachments being the most common.

All users shall adhere to the following when using the NCDC facilities to connect to the Internet:

a) During normal working hours, users must not use the Internet to access sites, or to download or upload information which is not specifically related to their job.
b) In case of disconnected gadgets, the users should report to the Systems Administrator as soon as possible so that the operations of the Centre are not affected.
c) Users who deliberately access sexually explicit images, store or make such images available on storage medium owned by NCDC will result in disciplinary action under NCDC's disciplinary procedures.
d) Users of Internet will not participate in chain letters; post statements that are defamatory or information that is false or misleading; or post confidential or proprietary information about NCDC or any of its stakeholders, staff and vendors on unsecured Internet sites such as bulletin boards, or disseminate such information in a way that might compromise its confidentiality.
e) Users will not make use of the Internet for any purpose which might be considered to contravene any existing laws of Uganda.
f) Users must always exit the Internet whenever work has been completed.
g) Users must never leave their desktop PC unattended when not at their workstation unless when using a time-out screen saver or logging out of the system.
h) Perceived breaches of security (actual or attempted) must be reported to the Systems Administrator who will regularly monitor and audit use of the Internet facilities to ensure that abuse is not occurring.
i) The Systems Administrator must hold up-to-date records of desktop PCs and all users permitted to access the Internet.
j) Users shall act ethically and responsibly in their use of the Internet and to comply with the relevant NCDC information security policy, regulations and codes of practice.
k) Users shall not post messages on newsgroups or chat areas that are likely to be considered abusive, offensive or inflammatory by others.
l) Users shall not use the NCDC Internet connection to attack other individuals or organisations.
m) Users shall be aware that the public nature of the Internet dictates that the confidentiality and integrity of information cannot normally be relied upon.
n) Software copyrights and license conditions shall be observed. Only licensed software shall be downloaded from the Internet and used.
o) All devices connected to the Internet shall be equipped with the latest and updated versions of anti-virus software.

3.4 Email Guidelines

The purpose of electronic mail (email) is to support business services throughout NCDC, by providing the ability to communicate quickly and effectively with both internal and external contacts. This policy governs the use of, access to and disclosure of email to assist in ensuring the NCDC's resources solely serve this purpose.

3.4.1 Use of Email

All users shall adhere to the following when using NCDC email facilities:

a) Users shall act ethically and responsibly while using emails and comply with NCDC ICT related policies, regulations and codes of practice.
b) Users shall not send messages that are likely to be considered discriminative, abusive, offensive, racist, and inflammatory by the recipient(s), or any messages that portray a bad image about the NCDC.
c) All users shall be aware that it is possible for the origin of an email to be easily disguised to appear to be coming from someone else.
d) Users shall not create or forward advertisements, chain letters or unsolicited emails e.g. spam.
e) Users shall exercise caution when providing their email addresses to others, and be aware that their email addresses could be recorded on the Internet.
f) All users shall be cautious when opening emails and attachments from unknown sources as these could be infected with viruses.
g) All emails or attachments that are encrypted or compressed shall be decrypted or decompressed and scanned for viruses by the recipient.
h) All security incidents involving email shall be reported to the Systems Administrator.
i) Users shall be aware that emails may be subject to audit by Systems Administrator to ensure that they meet the requirements of this policy. This applies to message content, attachments, and addresses to personal emails.
j) All official emails sent out by NCDC staff shall bear a confidentiality clause and a disclaimer which is approved by the Director.

3.4.2 Naming of email addresses

With NCDC portal already in place, all employees at NCDC shall be assigned NCDC customised email addresses of the form lastname.firstname@ncdc.go.ug or any other acceptable naming convention which is intuitive to staff.

3.4.3 Backup of emails

Email systems and other systems involved in the storage of email messages shall be "backed up" centrally and periodically. Personal emails shall be backed up on staff computers.
The backup however, shall be for NCDC administrative purposes only and it shall be the users' own responsibility to backup any of their emails they wish to retain for future reference.

3.5 NCDC Website

a) NCDC shall use its website (https://www.ncdc.go.ug) to communicate information regarding its services to all stakeholders. Some of the information to be posted on the website shall include; project progress updates and innovations to the public, invitations to tender, vacant posts, etc.

b) Whenever information is available for update onto the website, the update shall be authorised by the Director or his/her designate prior to uploading.

c) Where material owned by NCDC is published on the Internet, it must bear copyright markers.

d) Links to external sites should be verified to ensure that the link target page is valid, and is not presenting information likely to offend or prevent the inadvertent viewing of unsuitable material.

e) Information published by NCDC on the Internet must:
   i) not incite or promote illegal acts.
   ii) be legal, decent, honest and truthful.
   iii) not deliberately or negligently mislead the reader.
   iv) have a disclaimer attached to the document.

3.6 Intranet Services

It is NCDC policy to implement Intranet Service to provide quick and instant internal access to all NCDC documentation, which may include handbooks, policies, statements, news items, internal memos, downloadable files of all kind and any other documentation for internal use.

Intranet Services include facilities to design, develop and store information formatted as web pages and making them accessible through the LAN of NCDC, while Internet services publish information on the World Wide Web (e.g. information to external stakeholders). In general, both services use similar software and hardware technology.

Providing Intranet requires dedicated (application) software, such as Microsoft Internet Information Server. In general, this software is available as part of Server Operating Systems or may be acquired from third party vendors. A dedicated computer will be reserved for Intranet Services.

In its role as an intelligent conduit, NCDC will also set up an active portal that personalises information needs on logon and therefore facilitates easy access to appropriately packaged and relevant information targeted at specific stakeholders.

3.7 E-Governance

E-Governance may be defined as "the use of information technology to support government operations, engage citizens and provide government services". This broad definition encompasses four dimensions, which reflect the functions of government itself:

a) E-commerce: The exchange of money for goods and services over the Internet such as citizens paying taxes and utility bills, renewing vehicle registrations, and paying for recreation programs, or government buying office supplies and auctioning surplus equipment.
b) E-services: The electronic delivery of government information, programs and services often (but not exclusively) over the Internet.
c) E-management: The use of information technology to improve the management of government from streamlining business processes to improving the flow of information within government offices.
d) E-democracy: The use of electronic communication means, such as email and the Internet, to increase citizen participation in the public decision-making process.

E-Government will offer another way of serving citizens and will bring innovation to internal operations. While information technology may provide alternative methods for service delivery and government operations, it requires figuring out what to do within NCDC given the available resources, staff, priorities and constituents. It also requires re-assessing current business processes and functions in the government. The following are some of the benefits to be realised from the implementation of e-Governance:

i) Increasing efficiency by streamlining business processes
ii) Improving internal communication
iii) Providing better customer service
iv) Keeping up with citizens' demands and expectations

It is therefore a policy of NCDC to:

a) Use Internet for purposes of extending its services to the public and stakeholders. Such services may include: online delivery of teaching/learning materials, making inquiries on curriculum development issues, etc.
b) The services provided over the Internet must be in line with the National E-Government and Information Technology Policies.

4.0 SECURITY GUIDELINES

This section of the Policy defines the security controls necessary to safeguard NCDC ICT Systems and to ensure the security, confidentiality and integrity of the information held therein. It provides ways in which security threats to NCDC Information Systems can be identified and managed.

4.1 Scope

a) Password management
b) Incident Management
c) Physical and Environmental Security
d) Access to ICT equipment rooms
e) Transferring equipment offsite
f) Reporting of security incidents
g) Change Control
h) Encryption

4.2 Password Management

Usernames and passwords must be utilised to facilitate official access to the respective NCDC ICT resources. Their use protects NCDC's data from access by unauthorised individuals both internally and externally (hackers).

Passwords are an important aspect of computer security. They provide the top-most layer of protection for the entire ICT security environment. A poorly chosen password may result in the compromise of NCDC's entire ICT resources. As such, all users of NCDC ICT infrastructure (including contractors and vendors), must take responsibility when creating, using and sharing passwords.

The main purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords and the frequency of their change. With guidance from NITA Password Standard Policy Guidelines, the Systems Administrator will from time to time guide NCDC staff accordingly.

4.2.1 Password Security

The Systems Administrator and his/her supervisor will be the custodians of all NCDC System administrative Passwords.

4.2.2 Standard User Accounts

a) It is the responsibility of the Systems Administrator to provide access rights (usernames and passwords) to all authorised users of respective NCDC ICT systems.
b) All user-level passwords (e.g., email, web, desktop computer, etc) will be audited by the Systems Administrator periodically.
c) Passwords must not be inserted into email messages or other forms of electronic communication.
d) All user-level and system-level passwords must conform to the guidelines described below:
NCDC shall ensure that only users with valid user accounts are allowed to log onto the computer systems and where such systems are networked (or placed on a computer network), users shall be expected to use network user (domain) accounts to connect to their computers.

4.2.3 Admin Level Accounts

a) All Administrator-level passwords (e.g. Help desk, root, enable, MS Windows admin, etc) must be changed on at least a quarterly basis.
b) All production system-level passwords must be part of the ICT administered Active Directory Database (with exception of legacy systems).
c) User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.

4.2.4 General Password Selection Guidelines

Passwords are used for various purposes at NCDC. Some of the most common uses include: user level accounts, web accounts, email accounts, screen saver protection and banner logins. Since it is very easy to guess or crack certain types of passwords, everyone should be aware of how to select strong passwords.

1) Poor, weak passwords have the following characteristics:
   a) The password contains less than eight characters
   b) The password is a word found in the dictionary (English or Foreign)
   c) The password is a common usage word such as:
      i) Names of family, pets, friends, co-workers, fantasy characters, etc
      ii) Computer terms and names, commands, sites, companies, hardware, software
      iii) The words “entrepreneurship”, “Mbarara”, “Dubai” or any derivation.
      iv) Birthdays and other personal information such as addresses and phone numbers.
      v) Word or number patterns like aaabbb, QWERTY, 123456, zxcvb, etc. or any of the above words spelt backwards.

2) Strong passwords have the following characteristics:
   a) Contain both upper and lower case characters (e.g. a-z/A-Z)
   b) Have digits and punctuation characters as well as letters e.g., 0-9,!@#~*%^+-=><{}
   c) Are at least eight alphanumeric characters long
   d) Are not words in any language, slang, dialect, jargon, etc
   e) Are not based on personal information, names of family, etc.
   f) Passwords should never be written down or stored online. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation or other phrase. For example, the phrase might be: "This May Be One Way to Remember" and the password could be: "Asd@19Wq" or "R)aDgAE%" or some other variation.

4.2.5 Password Protection Guidelines

a) Do not use the same password for NCDC accounts as for other non-NCDC access (e.g., passwords of email, NSSF, insurance, URA, etc.). Where possible, don't use the same password for various NCDC access needs. For example, select one password for the network logon and a separate password for web mail systems.
b) Do not share NCDC passwords with anyone, including administrative assistants or secretaries.
c) All passwords are to be treated as sensitive and confidential NCDC information.
d) Avoid using the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger), where possible.
e) Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on any computer system without encryption.
f) Change passwords on a regular basis (except system-level passwords which must be changed quarterly). The recommended change interval is every six months.
g) If an account or password is suspected to have been compromised, report the incident to the Systems Administrator and change all passwords.

4.2.6 Password Ageing

Every NCDC officer shall have a password ageing policy to ensure that user passwords expire after a given period of time. Passwords shall not be used for a period exceeding six (6) months.

4.2.7 Password History

A password history shall be maintained for all domain levels. This history file shall be used to prevent users from reusing passwords. The history file shall minimally contain the last 23 passwords for each user name.

4.2.8 Unsuccessful Attempts to Enter a Password

To prevent password guessing attacks, the number of consecutive attempts to enter an incorrect password shall be strictly limited. After a defined number of unsuccessful attempts to enter a password (usually 3), the involved user account shall be suspended until the user requests for it to be reset by the Systems Administrator. Continued violation of this shall result in total disabling of the user account.

4.2.9 System Password Compromise

Whenever a non-authorised party compromises a system, the network/Systems Administrator or relevant ICT personnel shall immediately change every password on the involved system. Even suspicion of a compromise shall likewise require that all passwords be changed immediately. Under either of these circumstances, a trusted version of the operating system and all security-related software must also be reloaded and all recent changes to the user and system privileges shall be reviewed for unauthorised modifications.

5.0 INCIDENT MANAGEMENT GUIDELINES

The objective of this policy is to ensure that events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken. This clause describes a formal event reporting and escalation procedure for incident management at NCDC. All employees, contractors and third party users MUST be made aware of these procedures.

5.1 Reporting Information Security Events

A point of contact must be established for the reporting of information security events. It should be ensured that this point of contact is known throughout NCDC and is always available and is able to provide adequate and timely response.
All employees, contractors and third party users must be made aware of their responsibility to report any information security events as quickly as possible. They should also be aware of the procedure for reporting information security events and the point of contact.

The reporting procedures shall at least include:

a) Information security event reporting forms (see appendix 1) to support the reporting action and help the person reporting to remember all necessary actions in case of an information security event
b) Suitable feedback processes to ensure that those reporting information security events are notified of results after the issue has been dealt with and closed;
c) The correct behaviour to be undertaken in case of an information security event, such as:
    i) Noting all important details (for example type of non-compliance or breach, occurring malfunction, messages on screen, strange behaviour) immediately.
    ii) Not carrying out any individual action, but immediately reporting to the ICT Department.
    iii) Reference to an established formal disciplinary process for dealing with employees, contractors or third party users who commit security breaches in high risk environments.

5.2 Physical and Environmental Security

Physical and environmental security of ICT facilities is necessary to prevent their unauthorised use and to ensure that systems are adequately protected against natural hazards, theft and damage. Access to every office, computer room and work area containing sensitive information, or the means to access such information, shall be physically restricted. Rooms and facilities which house non-public IT resources shall be protected with physical security measures that prevent unauthorised persons from gaining access.

This control is aimed at offering the first line of defence for NCDC information and information processing facilities.

The following guidelines shall be considered and implemented where appropriate:

a) Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities like services and backup tapes, the strength of these security perimeters should be proportional to the value of assets it is protecting.
b) Perimeters of a building containing information processing facilities should be physically sound (such as there should be no gaps in the perimeter or areas where a break-in could easily occur).
c) External walls of the building should be of solid construction and all external doors should be protected against unauthorised access with strong control mechanisms, for example iron bars, alarms, locks.
d) Doors and windows should be locked when unattended.
e) External protection for windows on ground level should be implemented.
f) A manned reception to control physical access to the site or building should be improved through security awareness training.
g) Access to sites and buildings should be restricted to authorised personnel only.
h) All fire doors on a security perimeter should be alarmed, monitored and tested in conjunction with the walls to establish the required level of resistance in accordance with suitable national, regional and international standards.
i) Modern CCTV cameras may be installed around and within NCDC to improve security through surveillance.

5.3 Wi-Fi Security

It is NCDC Policy that any Wi-Fi Access Point (WAP) must be configured to comply with nationally accepted standards of reasonable wireless network security laws. The two main steps include:

a) Changing the WAP defaults (administration password, router name, router IP address, SSID name, etc)
b) Encrypting the signal using the best available encryption method, in the order -from most to least desirable: WPA2, WPA, 128-bit WEP.

6.0 ANTI-VIRUS AND SPAM GUIDELINES

Computer Viruses are small software programs that are designed to spread from one computer to another and to interfere with computer operations. Spam on the other hand is any kind of unwanted online communication, the most common form being unwanted e-mail.

Computer viruses impact productivity, incur financial costs and can result in the compromise or loss of data and reputation. Viruses can originate from a range of sources, spread rapidly and require comprehensive approach to ensure that the risks they pose are effectively managed. This comprehensive approach requires full cooperation of the staff of the respective NCDC offices.

6.1 Scope

a) Procurement of anti-virus software
b) Installation of anti-virus and updates
c) Administration responsibilities
d) Anti-virus implementation guidelines

6.2 Procurement of Anti-Virus Software

NCDC shall always procure corporate versions of the anti-virus, which will have been recommended by the Systems Administrator.

6.3 Installations of Anti-Virus and updates

a) The acquired anti-virus shall be installed on the respective NCDC Local Area Networks.
b) The installed software shall be programmed to make automatic updates from the Internet.
c) The workstations shall automatically pick the updates from the server.

6.4 Administration Responsibilities

The Systems Administrator shall have the responsibility to protect NCDC systems and ICT infrastructure from virus infection and to filter spam email by doing the following:

a) Evaluate, select, procure and deploy effective anti-virus software on file servers, desktops, laptops and other mobile devices to scan for viruses and Trojan horses.
b) Monitor systems regularly for devices that do not have antivirus software installed or have incorrect antivirus products or settings.
c) Provide a central point of contact to NCDC users for antivirus matters.
d) Keep abreast of potential viruses and Trojan horses that may affect NCDC.
e) Promote awareness of antivirus issues amongst users.

6.5 Anti-Virus Policy Implementation Guidelines

a) All users shall be on alert to the possibility of a virus and report any suspicious behaviour to the ICT Unit immediately.

b) All users shall ensure that their computer systems are installed with the approved antivirus software and that the software is up-to-date.

c) Users shall not install unapproved antivirus products, or try to alter the configuration or disable the existing anti-virus product.

d) Users shall ensure that all relevant software security updates are applied to their computers, e.g. using the Windows update service for all Microsoft operating systems, and the equivalent update service for other types of operating systems.

e) Users shall not open suspicious emails or attachments whether solicited or unsolicited from unknown or unusual sources.

f) In the event that a user is unable to clean or remove an infected file, the user shall disconnect the PC from the NCDC network by removing the network cable and inform the Systems Administrator of the problem immediately.

g) The Systems Administrator shall provide and maintain effective virus scanning and anti-spam measures at the NCDC gateway.

h) Users shall exercise caution when accessing web based emails, including but not limited to hotmail, gmail and yahoomail. Users shall be aware that emails accessed from these sites have not been scanned by the NCDC email gateway and may contain viruses.

i) All inbound and outbound emails from the NCDC network and all autonomous managed networks shall be centrally routed to ensure that uniform gateway virus scanning and spam filtering measures are applied.

7. DATA BACKUP AND DISASTER RECOVERY GUIDELINES

Data backup involves the saving of your data in two or more locations, so that if something happens to your computer, you still have your data reserved in backup. This allows you to keep your data even if you lose your computer.

7.1 Scope

a) Data Backup
b) Responsibility for data backup
c) Desktop backups

7.2 Data Backup

Regular back-up procedures are essential to guard against loss of data and software, and to facilitate a rapid recovery from any IT failure. This section of the ICT policy outlines guidelines for backing up NCDC data.
Information systems at NCDC shall provide backup and recovery features to guard against uncertainty:

a) Full backups for servers must be performed after every two days, from Monday to Saturday. If for any reasons, backups are not performed on a given day, they must be done on the morning of the following day.
b) Backups performed from Monday through Friday must be kept for one week and used again the following appropriate day of the week. The Systems Administrator shall perform regular backups.
c) The ability to restore data from backups shall be tested at least once a month.
d) The backups must be stored in an offsite location, at a sufficient distance to escape any damage from a disaster at the main site.
e) Backup information must be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site; the controls applied to media at the main site should be extended to cover the backup site.

NOTE: Training will be arranged for all staff to learn how to backup their documents.

7.3 Desktop Backup

All network users using personal computers/workstations and laptops must ensure that their data is backed up using one or a combination of the following methods:

a) Backing-up to a local device e.g. Zip Drive, CD ROM, USB Flash, or a portable hard disk

b) Copying critical data on a regular basis to a remote server that is properly backed up by NCDC
c) All users must always backup their data before updating

Appendix 1: ICT Fault Report Form

NCDC
NATIONAL CURRICULUM DEVELOPMENT CENTRE

ICT FAULT REPORT FORM

Use this form to report any ICT related problem(s) and incident(s). Return completed form to the Systems Administrator.

Staff Name: …… Designation .....

Department …….... Date Reported ……..……

Time ……....

Problem Description: .....…

……..……..……..

FOR USE BY ICT STAFF ONLY

Date Received …… Time ……..

Problem Observed: .....

.....

Action Taken:

	STATUS
	Complete
	Incomplete
	Under Observation
	Beyond Repair

Recommendation and Signature:

. .....

.....

..... Date Completed: .....

Appendix II: ICT Committee Establishment

NCDC ICT Committee Terms of Reference

Establishment
The ICT committee is established by the Director of National Curriculum Development Centre (NCDC). The five (5) member Committee, responsible to the Director, includes the following;

1) Head of ICT Department (Chairperson)
2) Deputy Director
3) Finance Secretary
4) Librarian
5) Systems Administrator (Secretary)

NOTE: The ICT Committee has powers to co-opt additional members for purposes of subject specific information or as may be deemed necessary.

Committee Chairperson
The Chair will be the Head of the ICT Unit. The Chair will ensure that the ICT Committee undertakes its responsibilities and meet its objectives. The Chair may appoint an interim Chair from time to time; in such cases, the duration of tenure shall be specified.

Functions
This Committee shall provide advice to the office of the Director to:

a) align and coordinate Information and Communication Technology (ICT) investments with the institution's strategic priorities to eliminate duplication.
b) monitor and support ICT-related projects and investments at the Centre and report on performance as required.
c) monitor benefits arising from ICT investments and ensure their full realisation.
d) monitor and make recommendations on risks associated with ICT investments.
e) oversee the implementation of the NCDC ICT Policy.

Responsibilities

a) Ensure that the NCDC's ICT resources are aligned to its stated strategic aspirations
b) Oversee development and support of major ICT systems and functions
c) Recommend the ICT strategic plan, policies and support compliance initiatives to management for approval
d) Develop and champion principles that will guide and govern decisions around ICT at the Centre Guide strategic ICT decisions with respect to both ICT architecture and investment
e) Monitor performance of ICT services and investments at the Centre
f) Ensure that ICT management policies and procedures are established and

implemented in accordance with government ICT policies

g) Approve ICT investments
h) Provide key input into the NCDC's planning and budgeting process on ICT infrastructure development
i) Communicate and engage with the NCDC community about emerging issues in the area of ICT
j) Advise management on any matters of ICT they wish to draw attention to and deemed appropriate
k) Endorse the ICT Strategic Plan
l) Ensure strategic alignment of ICT investment decisions with NCDC and government priorities

Meeting and Voting

a) The Committee will meet quarterly or as and when there is need.
b) Meetings will be conducted at a place determined by the Chair.
c) Meetings will be conducted on a formal basis and be minuted.
d) A quorum shall comprise at least three (3) members of the ICT Committee with the Chairperson inclusive (60% of the membership).

Agenda

a) An agenda is to be prepared for meetings with relevant issue papers attached and distributed to members, preferably at least 48 hours prior to the meetings.
b) Agenda items may be considered out of session by electronic or other means and should be minuted at the next available meeting.

Minutes

a) Minutes of the meeting must be forwarded to members within 2 weeks before the next meeting
b) The minutes must record the following:
    - Date and location of meeting
    - Attendees, apologises and absentees
    - Agenda items discussed
    - Action items (including responsibility and timeframe)
    - Decisions taken (including rationale for decisions)
c) Minutes of the preceding meeting must be confirmed at each meeting, which includes a review of the action items outstanding.
d) The minutes must be approved by the Chair.

Once approved, the minutes of the meeting will be shared with all members.

National Curriculum
Development Centre ,
P.O. Box 7002,
Kampala.
www.ncdc.go.ug