1.0 PURPOSE

This guideline provides a framework for the management of information Communication Technology (ICT) in Africa International College and Africa Community School Abuja. It applies to:

a. All those with access to the School Information Systems, including staff, students, visitors and contractors;
b. Any systems attached to the School computers or telephone networks and any systems provided by the School;
c. All information (data) processed by the Schools pursuant to its operational activities, regardless of whether it is processed electronically or in paper (hard copy) form, any communications sent to or from the School and any School information (data) held on systems external to the School's network;
d. All external parties that provide services to the School in respect of information processing facilities and business activities; and
e. Principal information assets including the physical locations from which the School operates.

2.0 AIMS AND COMMITMENTS

a. The School recognizes the role of information security in ensuring that users have access to the information they require in order to carry out their work. Computer and information systems underpin all the School's activities, and are essential to its teaching and administrative functions.
b. Any reduction in the confidentiality, integrity or availability of information could prevent the School from functioning effectively and efficiently. In addition, the loss or unauthorized disclosure of information has the potential to damage the School's reputation or cause financial loss or other negative effects.

c. To mitigate these risks, information security must be an integral part of information management, whether the information is held in electronic or hard-copy form.
d. The School is committed to protecting the security of its information and information systems in order to ensure that:
    i. Information is always available to those who need it and there is no disruption to the business of the School;
    ii. The School meets its operational obligation including those applicable to personal and academic data.
    iii. The reputation of the School is promoted and safeguarded.
e. In order to meet these aims, the School is committed to implementing security controls that conform to best practice at all times. The School will draw and update information security toolkit guidance on the information communication.
f. Information security risk assessments will be performed for all information system on a regular basis in order to identify key information risks and determine the controls required to keep those risks within acceptable limits.
g. The School is committed to providing sufficient education and training to users to ensure they understand the importance of information security and in particular, exercise appropriate care when handling confidential information.
h. Specialist advice on information security shall be made available to teachers and other support staff that handle critical data and information.
i. An information security advisory group (or groups), comprising representatives from all relevant parts of the School, shall advise on best practice and coordinate the implementation of information security controls.
j. The School will establish and maintain appropriate contacts with relevant organizations, network and telecommunications operators in respect of its information communication system.
k. Breaches of information security must be recorded and reported to appropriate school authority who will take appropriate actions immediately.

l. This guideline and all other supporting guidelines circulars shall be communicated as necessary throughout the School to meet its objectives and requirements.

3.0 RESPONSIBILITIES

The school authority has ultimate responsibility for information security within the School. More specifically, it is responsible for ensuring that the School uses its ICT facilities to the optimum and promote efficiency and productivity in all areas.

3.1 Head of ICT Department

The Head of the ICT unit, or any future equivalent body, is responsible to the school authority for:

a. Ensuring that users are aware of these guidelines;

b. Seeking adequate resources for its implementation;

c. Monitoring compliance;

d. Conducting regular reviews of the guidelines, having regards to any relevant changes to other School guidelines and or obligations;

e. Ensuring there is clear direction and visible management support for ICT initiatives.

3.2 Heads of department/class teachers/unit heads

Given the School's structure, teachers, heads of department and non-teaching staff are responsible for information security within their departments. They must ensure that their office has in place, a local information guideline to meet its own particular needs consistent with the requirements of this overarching guideline. The local information security guidelines should identify the

department's own information security requirements and provide a management framework for meeting those requirements

Specific roles and responsibilities for information security within department must be clearly identified.

They must approve the internal guidelines, and ensure that it is implemented and kept under regular review.

3.3 Users and External Parties

All users of School information should be aware of their own individual responsibilities for complying with the School and departmental guidelines on Information Communication Technology (ICT) facilities.

Agreements with third parties involving accessing, processing, communicating or managing the School's information, or information systems, should cover all relevant security requirements and be covered in contractual arrangements.

4.0 RISK ASSESSMENT

4.1 Risk assessment of information held

The degree of security control required depends on the sensitivity or criticality of the information. The first step in determining the appropriate level of security therefore is a process of risk assessment, in order to identify and classify the nature of the information held, the adverse consequences of security breaches and the likelihood of those consequences occurring.

Given the nature of the School's structure, the risk assessment should be carried out in the first instance by departments. The departmental assessment must be consistent with the general principles in this section.

The risk assessment should identify the department's information assets, define the ownership of those assets and classify them according to their sensitivity and/or criticality to the department or School as a whole. In assessing risk, departments should consider the value of the asset(s), the threats to that asset and its vulnerability. Where in doubt, the school authority should be contacted to obtain written guideline or approval.

Where appropriate, ICT assets should be labeled and handled in accordance with their criticality and sensitivity.

Rules for the acceptable use of ICT assets should be identified, documented and implemented. The School's Regulations and Guidelines applying to all users of the facilities can be obtained on request.

Information security risk assessments should be carried out regularly as required during the operational delivery and maintenance of the School's infrastructure, systems and processes.

4.2 Academic Data

Academic data must be handled in accordance with the standard professional care and in compliances to the School's guidelines and guidance on academic data.

The OPA requires that appropriate technical and organizational measures are taken against unauthorized or unlawful processing of academic data, against accidental loss or destruction of, or damage to the data.

A higher level of security should be provided for 'sensitive, personal and academic data', which include data relating to scores, bio data, and physical health information obtained during counseling or other personal confidential matters.

5.0 PROTECTION OF SYSTEMS AND ASSETS

Having completed a risk assessment of their ICT assets, departments/units should draw up their own information security guidelines, setting out appropriate controls and procedures. The head of department or unit must be satisfied that the controls will reduce any residual risk to an acceptable level, in line with standard practices.

Confidential information should be handled in accordance with the requirements set out in section 6 below.

6.0 PROTECTION OF INFORMATION AND DATA

6.1 Significant and classification

a. Identifying confidential information is a matter for assessment in each individual case.
b. Broadly, however, information will be confidential if it is of limited public availability; is confidential in its very nature; has been provided on the understanding that it is confidential; and/or its loss or unauthorized disclosure could have one or more of the following consequences: financial loss, breach of confidence; reputational damage, adverse publicity, complaints about breaches of privacy; and/or an adverse effect on the safety or well-being of members of the School or those associated with it e.g. increased threats to staff or students, embarrassment or damage to benefactors, suppliers, staff and students.
c. For AIC, the following data or information are confidential: Biodata, scores, students or staff assessment, examination questions and answers, information extracted during counseling, staff confidential records and financial data etc.

6.2 Storage

Confidential information should be kept secure, using, where practicable, dedicated storage (e.g. file servers) rather than local hard disks, and an appropriate level of physical security.

File or disk encryption should be considered as an additional layer of defense, where physical security is considered insufficient.

a. Wherever practicable, documents with confidential information should be stored in locked cupboards, drawers or cabinets. In addition, the room, information should be kept should be locked when unoccupied for any significant length of time.
b. Keys to cupboards, drawers or cabinets should not be left on open display when the room is unoccupied.

6.3 Access

Confidential information must be stored in such a way as to ensure that only authorized persons can access it.

All users must be authenticated. Authentication should be appropriate, and where passwords are used, clearly defined guidelines should be in place and implemented. Users must follow good security practices in the selection and use of passwords.
Where necessary, additional forms of authentication should be considered.

a. To allow for potential investigations, access records should be kept for a minimum of six months, or for longer, where considered appropriate.
b. Users with access to confidential information should be security vetted, as appropriate.
c. Physical access should be monitored, and access records maintained

6.4 Remote access

Where remote access is required, this must be controlled via well-defined access control guidelines and tight access controls provided to allow the minimum access necessary.

Any remote access must be controlled by secure access control protocols using appropriate levels of encryption and authentication.

6.5 Copying

The number of copies made of confidential information, whether on portable devices or media or in hard copy, should be the minimum required, and, where

necessary, a record should be kept of their distribution. When no longer needed, the copy should be deleted or, in the case of hard copies, destroyed.

All copies should be physically secured e.g. stored in a locked cupboard drawer filing cabinet or fire proof safe, as the case may be.

6.6 **Disposal**

All data or information budget required must be securely or destroyed by the appropriate person. In the case of old computers other devices, they must properly be cleaned off (all other devices, must be properly cleaned off and all data information deleted before they are destroyed or disposed of.

Confidential documents must be shredded in a confidential manner prior to disposal.

7.0 USE OF PORTABLE DEVICES OR MEDIA

(a) All portable devices or removable media must be screened by the Head of ICT Unit in order to ensure that the systems are appropriately protected from unauthorized access and infections.

(b) No printing of personal documents will be allowed in the unit.

(c) The permission of the officer in charge must be sought before ICT devices are moved off site. The officer in charge must be satisfied that the removal is necessary and that appropriate safeguards are in place.

(d) Installation of personal software's or devises by any user is prohibited.

(e) No part of the systems should be pass worded by any student or staff, passwords must be provided by the Head of the unit.

(f) Once a password is provided, it is the responsibility of the officer or user to ensure the passwords remain confidential under their care.

(g) In the case of student data or personnel information, all portable devices and media should be encrypted where the loss of the data could cause damage or distress to the School.

(h) The passphrase of an encrypted device must not be stored with the device.

8.0 EXCHANGE OF INFORMATION AND USE OF EMAIL

Controls should be implemented to ensure that electronic messaging is suitably protected.

Email(s) should be appropriately protected from unauthorized use and access.

Email(s) should only be used to send confidential information where the recipient is trusted, the information owner has given their permission, and appropriate safeguards have been taken e.g. encryption. Additional guidance on managing the risks associated with the use of e-mail must be applied.

a. If confidential documents are sent by fax, the sender should ensure they use the correct number and that the recipient is near to the machine at the other end ready to collect the information immediately it is printed.
b. If confidential documents are sent by external post, they should ideally be sent by a form of recorded delivery. The sender must ensure that the envelope is properly secured.
c. If confidential documents are sent by internal post the documents should be placed in an envelope marked 'Confidential' with the addressee's name clearly written on it.
d. If documents are sent by hand, it must be through the staff affected Or a reasonably senior staff.

9.0 SYSTEM PLANNING AND ACCEPTANCE

A risk assessment should be carried out as part of the business case for any new ICT system that may be used to store confidential information. The risk assessment should be repeated periodically on any existing systems.

10.0 BACKUP

Users should ensure that appropriate backup and system recovery procedures are in place. Backup copies of all important information assets should be taken and tested regularly in accordance with an appropriate backup requirement.

11.00 HARD COPIES

Protective marking

Documents containing confidential information should be marked as 'Confidential' or with another appropriate designation e.g. 'sensitive', etc., depending on the classification system adopted by the department.

12.00 **REMOVAL**

Confidential information should not be removed from the School without written approval.

13.0 **ENFORCEMENT**

- Any failure to comply with the guidelines may result in disciplinary action.
- Any loss, damage or unauthorized disclosure must be promptly reported to the head of department/unit and to the appropriate school authority. Anyone, staff or student responsible for any loss or damage will be held responsible.
- Computer security incidents involving the loss or unauthorized disclosure of confidential information held in electronic form must be reported to the appropriate authority and investigated.
- If the loss or unauthorized disclosure involves personal data, whether electronic or hard copy, the school authority must also be informed immediately.

14.0 **COMPLIANCE**

The School has established these guidelines to promote information security and compliance with other relevant rules and procedure of AIC. The School regards any breach of information security requirements or unauthorized access to its ICT facilities as a serious matter, which may result in disciplinary action and or legal actions.

Compliance with these guidelines should form part of any contract with a third party that may involve access to network or computer systems or data of the School.

15.0 **LINKAGE WITH OTHER GUIDELINES**

This set of regulations on the ICT facilities should be read and applied along with relevant portions of other Handbooks, guidelines ad manuals published by the School.

16.0 AMENDMENTS AND CHANGES

The School authority reserves the right to make changes to these rules and guidelines at any time and such changes shall have the same effect as all other parts or sections of this manual.

17.0 DEFINITIONS

Access Control - Ensures that resources are only granted to those users who are entitled to them.

Appropriate - Suitable for the level of risk identified and justifiable by risk assessment.

Asset - Anything that has a value to the School

Audit - Information gathering and analysis of assets to ensure such things as guidelines compliance and security from vulnerabilities.

Authentication - The process of confirming the correctness of a claimed identity.

Best Practice - Current standard advice for implementing security controls. Synonymous with 'good practice'.

Confidentiality - Confidentiality is the need to ensure that information is disclosed only to those who are authorized to view it.

Control - A means of managing risk by providing safeguards. This includes guidelines, procedures, guidelines, other administrative controls, technical controls or management controls.

Data - Information held in electronic or hard copy form.

External Party - see 'Third Party'

Information - Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

Information Owner - Synonymous with 'information risk owner'. This is the person who is responsible for accepting any residual risk.

Information Security - Preservation of confidentiality, integrity and availability

Information security toolkit - Collection of guidelines, guidelines, interpretation, technical guidance and example solutions.

Information Systems - Any system, service or infrastructure used to process information or the physical locations housing them. This includes critical business environments, business processes, business applications (including those under development), computer systems and networks.

Personal Data - Any data held in a system, whether electronic or hard copy, that identifies.

Guidelines - overall intention and direction as formally expressed by management

Risk - the potential for an unwanted event to have a negative impact as a result of exploiting a weakness. It can be seen as a function of the value of the asset, threats and vulnerabilities

Risk Assessment - Overall process of identifying and evaluating risk.

Third party - person or body that is recognized as being independent of the School.

Threat - Something that has the potential to exploit a weakness to result in some form of damage. Threats can be environmental, deliberate, accidental, logical or technical.

Vulnerability - Weakness of an asset or group of assets that may be exploited by a threat.