THE INSTITUTE OF ADULT EDUCATION

IAE POLICY FOR THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGY (ICT)

POLICY No: IAE/ICT/2013/01
EFFECTIVE: 2013/14 (Financial year)

TABLE OF CONTENTS

Preface

The IAE cannot afford to overlook the importance of Information and Communication Technology (ICT) for improved access, equity, quality and relevance education for its students and staff. The ICT environment is dynamic and that rapid technological development would change among other things, how we communicate and access information and services.

This ICT policy framework therefore focuses on addressing among other things; ICT infrastructure, ICT security, E- mail services, capacity building and Training, maintenance and technical support in ICT facilities while ensuring that the IAE community benefits from new services offered by the ICT, and that technologies are used to meet the development goals of the IAE.

The benefits of ICT can only be reaped through the commitment and collaboration of all ICT stakeholders. That is why other ICT stakeholders were consulted in development of this policy.

This policy constitutes an integral part of the long- term vision, Mission and strategic plan and objectives of the institutes. The IAE is convinced that this policy will serve as basis for the ICT demand so that it can become an efficient, responsive and result oriented.

I hope that This ICT policy provides comprehensive framework for the betterment of the Institute.

Prof Elifas Bisanda

Council`s Chairperson

Institute of Adult Education

1.0 INTRODUCTION

The IAE is a public service institution established under Act No. 12 of 1975. The IAE is one among the institutions under the Ministry of Education and Vocational Training (MoEVT). It is responsible for training adult educators, teachers/facilitators and administrators of adult education. It provides education through Open and Distance mode of learning and mass campaigns on diverse cross-cutting issues.

Other functions of the IAE are to conduct research and evaluation of adult education, to provide consultancy in adult education and open distance learning programmes. In view of the charged functions stated above, in this institution Information and Communication Technology (ICT) system carries a critical role in both administrative and academic matters in real time. In order to discharge its functions and to achieve its goals smoothly, ICT has become the backbone of day to day operations at the IAE.

2.0 RATIONALE OF THE POLICY

Information Technology resources are valuable assets and critical mechanism provided to enhance the core functions of the IAE. The acceptable use of information technology resources policy governs the use of the Institute's information technology resources in an atmosphere that encourages free exchange of ideas and an unwavering commitment to academic freedom. ICT policy will enhance proper, effective and sustainable use of ICT facilities at IAE.

2.1 Vision of the Policy

Seeing the IAE as a centre of excellence that maintains a learned and informed society.

2.2 Mission of the Policy

Enhancing IAE in developing, designing and implementing quality Adult and continuing education training programmes that will enable people acquire knowledge and skills required for sustainable development and dealing with global challenges.

2.3 Goal

The general aim of this policy is to ensure that ICT is entirely integrated into planning and implementation of the institute's mission as stipulated in the Corporate Strategic Plan in order to improve quality of activities at the Institute of Adult Education.

2.4 Objectives

To achieve the goal of this policy the Institute has to:

1. Develop and Improve ICT infrastructure,
2. Strengthen ICT security,
3. Provide electronic mail services to all staff and other policy beneficiaries,
4. Enhance installation, maintenance and technical support in ICT facilities,
5. Establish Guidelines for capacity building and Training for ICT professionals,
6. Control procurement of ICT facilities/equipments
7. Enhance efficient use of information system by the target group
8. Set up an independent ICT management structure, and
9. Enhance integration of ICT in teaching, learning and administration.

3.0 POLICY SCOPE

3.1 Resources Covered

This policy applies to all Institute ICT resources. It therefore, applies to computers and communication facilities owned, leased, operated or provided by the Institute or otherwise connected to Institute ICT resources. These include, but not limited to, networking devices, email system, database and information systems, servers, operating systems, personal digital assistants (PDAs), telephones, wireless gadgets, personal computers, workstations, minicomputers, printers and copiers and any associated

peripherals and software whether used for administration, research, teaching or other purposes.

This policy also applies to all personally owned devices used to store, process or transmit Institute's information or that are otherwise connected to Institute's ICT resources.

3.2 Individuals Covered

This policy applies to the entire staff, students and others referred to as users throughout this policy while accessing, using or handling the IAE's ICT resources. In this policy, "users" include but are not limited to sub-contractors, dignitaries, visitors, visiting scholars, students, research associates, grant and contract support personnel, media representatives, guest speakers, and non-Institute entities granted access.

4.0 COMPLIANCE (PRECAUTIONARY AND DISCIPLINARY MEASURES)

Deliberate and serious breach of the policy statements in this section will lead to disciplinary measures which may include the offender being denied free access to computing facilities and subjected to compensation as per damage costs. In addition to that, at minimum, individual Institute's units (such as campuses or institute's departments, regional centres and divisions) must follow these principles and rules while connected to Institute's ICT resources. Each unit is responsible for security on the entire ICT system of the Institute. A unit may apply more stringent security standards than those detailed here, provided these do not conflict with or lower standards or requirements established by any other related Institute's policies.

5.0 COPYRIGHT AND LICENSES

Take care to use software legally in accordance with the relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges. Furthermore, violation of copyright law or infringement is prohibited by Institute policies

and the Government laws. Generally, only the owner of a copyrighted work may reproduce, create other works based on the copyrighted work, distribute, perform, or publically display a copyrighted work. Any unauthorized use of copyrighted material including unauthorized peer-to-peer file sharing, may subject the user to discipline as a violation of one or more provisions of the general standard of conduct in the student's handbook or to discipline under the Code of Conduct in the Human Resources Policy and Procedures.

While the Institute has deployed and desires to maintain various technologies that actively prohibit copyright infringement activities, the Institute does not actively monitor its system network for copyright infringement, but does investigate all complaints or notices. In the event that the Institute receives the notice on a potential copyright violation, the IAE is obliged to investigate all matters related to complaints or notices.

5.1 Institute's Rights

Users should be aware that any activity on systems and networks may be monitored, logged and reviewed by the Institute approved personnel or may be discovered in legal proceedings. All documents created, stored, transmitted or received on Institute's computers and networks may be subject to monitoring measures by systems administrators.

The Institute reserves the right to access, monitor, review and release the contents and activity of an individual user's account(s) including emails; on any account; on any Institute-owned or non-Institute-owned resource; and on or off Institute's property connected to Institute's networks. This action may be taken to maintain the network's integrity and the rights of those with authorized access, to safeguard against threatened security of a computer or computers network system, to protect from other suspected misuse of Institute's resources, or to respond to the legitimate business needs of the Institute. Prior approval from the IT Security Office or another authorized Institute's office (such as the Office of Director General, Audit and Consulting Services) or court order must precede this action.

5.2 User Privacy

The Institute provides electronic resources to users to help the IAE fulfil its mission. The Institute routinely monitors electronic data, hardware, software and communication patterns. There should be no expectation of any attempted deed to have a room for privacy for any information stored, processed or transmitted on Institute's ICT resources.

As required by the Government of the United Republic of Tanzania law, the Institute hereby notifies users that emails may be a public record and open to public inspection under the IAE Act, unless the email is covered by an exception to the Act, such as personally identifiable student information, proprietary information or trade secrets.

6.0 POLICY ISSUES AND STATEMENTS

6.1 ICT Infrastructure

a) Hardware

ICT infrastructure refers to computers, computer peripherals, printers, scanners, hubs, switches, routers, servers, networking cables, etc. The purpose of this institutional infrastructure policy is to provide procedures and guidance for the proper acquisition, installation and maintenance of ICT equipment. Users shall follow the ICT equipment acquisition, installation and maintenance policy in this document.

b) Software

ICT infrastructure also refers to software in use by IAE that has been developed by IAE staff, local vendors or purchased from local or international vendors. The purpose on this issue is to provide procedures and guidance for the proper acquisition, installation and maintenance of software.

Policy Statement

All requests for a new application/system software enhancement must be presented to the ICT Unit with the user requirements presented in a User's Requirements Specification document. In addition to that, Hardware and

Software purchases should be approved by the ICT steering Committee preferably through the approved budget framework.

1. In the case of Installing Software, users should get permission from the ICT help desk before installing any software on equipment owned and/or operated by the IAE.
2. All software packages running on IAE's infrastructure must be compatible with the IAE's preferred and approved computer operating system and platform as set by the ICT Office from time to time.
3. Installation of new or upgraded software shall be done in consultation with the ICT Office. The ICT Office shall ensure that such installations are carefully planned and managed and IT security risks associated with such software are mitigated using a combination of procedural and technical control techniques.
4. The decision whether to upgrade software shall only be taken after the consideration of the associated risks of the upgrade and weighing these against the anticipated benefits and the necessity for such a change.
5. Do not take food or drink into rooms which contain specialized equipment like servers. Access to such rooms is limited to systems administrators and other authorized members staff.
6. Do not re-arrange how equipment is plugged in (computers, power supplies, network cabling, modems, etc.) without first contacting IT Support.
7. Technical audits shall be undertaken at least every three years by the ICT Office to determine the performance of computers and recommendations shall be made for replacement or otherwise.

6.2 ICT Security

Security and safety is about protection of ICT infrastructure, data and the user community against attacks from internal or external sources. Relevant policies need to be put in place to ensure protection of users and ICT

facilities like computer rooms, workstations, servers, switches, hubs, routers, firewalls, network wiring systems and other small or large ICT devices.

Deliberate attempts to degrade the performance of the IAE network or to deprive authorized personnel of resources or access to any IAE facilities is prohibited. Breach of security includes, but not limited to, the following: creating or propagating viruses, hacking, password grabbing, disc scavenging, etc. The IAE shall give high priority for preventing threats from being materialized and therefore users are required to adhere to this security and safety policy.

Policy statement

1. All IAE's computer hardware shall be marked, either by branding or etching with the name of the IAE and name of the office or computer laboratory where the equipment is normally located.
2. The IAE shall identify and isolate secured areas (such as server rooms) from physical contact or access. Secured areas shall be entered only by the authorized personnel.
3. During non-working hours, secure areas shall be protected against intrusion by appropriate access control, locks, and surveillance systems or by security personnel.
4. The IAE shall put signs or sign board labelled as "Authorized Personnel Only" in areas where there is physical access restriction.
5. Only authorized personnel are permitted on record to take computerized equipment belonging to the IAE off the premises and they are responsible for its security and safety.
6. Firewalls and Intrusion Detection systems shall be used across the entire organization network to monitor and prevent hackers, viruses and worms including all other forms of attach. The in-charge of network shall ensure that this policy is adhered to. Failure to do this may necessitate disciplinary action depending on circumstances and top management approval. All computers hooked into the network shall mandatorily have up-to-date antivirus software to prevent viruses and all other forms of malicious code. Additionally, the computers must have all

unnecessary services disabled to prevent intrusion. All members of staff are also expected to seek authority from ICT support before hooking any laptop to the network. They are also expected to timely report outdated versions of antivirus for action to IT help desk.

6.3 Electronic Mail (Email)

Email service is one of the major services on the IAE. The IAE shall provide email services on its network to support its academic and administrative functions to all users. In order to enable users share information, improve communication, exchange ideas and improve productivity, the institute encourages the use of email. For proper usage of the email service, users are required to firmly follow this email.

The contents of email messages sent or received are generally intended to be confidential.

This policy covers appropriate use of any email sent from a IAE email address and applies to all employees, vendors, and agents operating on behalf of the Institute.

Policy Statement

1. Prohibited use, the IAE email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any IAE employee should report the matter to the ICT unit, human resource department or to their supervisor immediately.

2 Personal use, using a reasonable amount of IAE resources for personal emails is acceptable, but non work related emails shall be saved in a separate folder from work related emails. Sending chain letters or joke emails from the IAE email account is prohibited. Virus or other malware warnings and mass mailings from IAE shall be approved by IAE system administrator or any other relevant authority before sending. These

restrictions also apply to the forwarding of mail received by the IAE employee.

3. Monitoring, IAE employees shall have no expectation of privacy in anything they store, send or receive on the Institute's email system. The IAE may monitor messages without prior notice. On the other hand the IAE is not obliged to monitor email messages
4. Enforcement, any employee found to have violated this policy may be subject to disciplinary action up to and including termination of employment.

6.4 Enhancement of ICT Installation, Maintenance and Technical Support

Maintenance of ICT systems requires specialist knowledge, skills and experience, involving technical and contractual issues specific to the ICT. The risks associated with poor or unplanned maintenance of ICT equipment might include; Potential implementation delays of services, incorrect ICT solutions, Inability to deliver services to IAE beneficiaries.

Policy Statement

1. All ICT technical assistance requests shall be channelled through the centralised helpdesk system. Requests and/or complaints made through other means e.g. telephone shall be given less priority than requests made through the helpdesk system.
2. Maintenance and support of all ICT facilities should be carried out by the IAE's ICT responsible unit. For maintenance and support, all networked servers are to be situated at the IAE's main data centre.
3. Deliberate or accidental damage to the IAE's ICT property shall be reported to the ICT help desk / officer in charge of ICT as soon as it is noticed.
4. All ICT equipment owned, leased or licensed by the IAE shall be supported by appropriate maintenance facilities by qualified technicians.

5. Adequate resources shall be made available for a regular maintenance of ICT equipment.
6. Computing services shall continue to be provided with strong user support to ensure integrated access to information services.

6.5 Guidelines for Capacity Building and Training for ICT Professional

Information and communication technology (ICT) is increasingly having pervasive role and presence in the educational sector as it continues to shape all aspects of daily lives. Numerous reforms should be in place aiming to infuse ICT across education systems. Facilitators are widely believed to be the key agents of any educational changes. ICT training courses, seminar, and workshops are vital aiming to prepare facilitators to integrate ICT effectively across the curriculum. ICT professional development courses for academic and non academic staff should be in place helping them to improve their ICT skills and knowledge.

Policy Statement

1. Every section within ICT Unit shall identify training needs at every beginning of financial year and forward to the ICT steering committee.
2. The ICT steering committee shall analyse the trainings relevance for every section to make sure that the training requirements are relevant to the staff and within budget and forward the names and requirements to higher authority for approval and needful action.
3. The superior in charge of ICT shall, upon his approval, forward the training requirements to Human Resource and Administration for implementation.
4. It shall be mandatory for all IAE staff to be literate users of ICT services, the level of literacy being in line with the demands of their job functions.
5. Computer literacy programmes shall be offered to the IAE community with the objective of not only ensuring user satisfaction but also reducing the user support load on the involved ICT personnel.

6.6 Procurement of ICT Facilities/Equipment

Comprehensive plan and well analyzed budget framework have to be prepared to meet ICT prospective demands. Therefore, the procurement of all ICT related devices and computer accessories has to be done in accordance with the Procurement Act No. 1 of 2004 rules and regulations as amended in 2007; National ICT policy; and IAE ICT policy as issued from time to time.

Policy statement

1. The IAE ICT steering committee has to approve all recommendations and specifications as proposed by the IT unit pending any procurement process of ICT devices and accessories to be implemented. The ICT steering committee has to exactly countercheck if the reliable vendors accordingly comply with the given recommendations and specifications before the acceptance of any ICT related devices and accessories delivery. The ICT steering committee has to involve all ICT specialists and experts from different fields of specializations to enable the Institute of Adult Education procure the right choice and only acceptable ICT related devices and accessories according to specifications proposed. All decisions regarding ICT procurement in general, have to be made in time in order to meet any rapid global technological changes and demands.
2. All regional campuses/centres should submit their ICT requirements to the ICT at headquarters for analysis and evaluation to ensure standards, compatibility and maintainability.

6.7 Use of Information System by Target Group

Information system involves complementary networks of hardware and software used to collect, filter, and process, create, and distribute data. It aims at supporting operations, management and decision making hence, requires technical guidelines, procedures and precautions to ensure usability, compatibility and maintenance of all ICT systems and gadgets.

Policy Statements

1. All servers shall have anti-virus software installed and a form of monitoring to ensure that only authorized users have access.
2. Users shall;
    a. Comply with Institute's policies and follow Institute's best practices where possible to maintain the confidentiality, integrity; and availability of computer systems and information on all devices and accessories under their control.
    b. Make regular back-ups of information and files as much as appropriately possible.
    c. Control and secure physical and network access to ICT resources and data.
    d. Properly log out of system sessions.
    e. Monitor access to their accounts. If a user suspects unauthorized activity or that their accounts have been compromised, they must report the matter to the responsible ICT personnel and change passwords immediately.
    f. Install, use, and regularly update virus protection software.
    g. Where technically possible, abide by the password protection best practices specified for each ICT resource.
    h. Use only the passwords and privileges associated with their computer account(s) and use those account(s) only for their authorized purposes.
    i. Respect and honour the rights of other individuals with regard to intellectual property, privacy, freedom from harassment, academic freedom, copyright and use of ICT resources.
    j. Use the Institute's provided software in a manner that strictly adheres to all licensing provisions, including installation, use, copying, number of simultaneous users and other terms of the license.
3. Users will not:

a. Provide access codes to any unauthorized user.

b. Use accounts, access codes, privileges or ICT resources for which they are not authorized.

c. Tamper with, modify, or alter any restrictions or protections placed on their accounts, the Institute's system or network facilities.

d. Physically damage or vandalize ICT resources, or use ICT resources to damage other Institute's resources or systems.

e. Commit copyright infringement including file sharing of videos, audios, or data without prior permission from the copyright owner.

f. Use ICT resources to introduce, create or propagate computer viruses, worms, Trojan horses, or other malicious codes.

g. Obtain extra ICT resources or gain access to accounts for which they are not authorized.

h. Snoop on or intercept other users' transmissions.

i. Attempt to degrade the performance or availability of any system or to deprive authorized users' access to any Institute's ICT resources.

j. Misrepresent their identities with actions such as Internet Protocol (IP) address "spoofing," email address falsification or social engineering.

k. Send email chain letters or mass mailings for purposes other than official Institute's related business.

l. Use Institute's resources to relay mail between non – IAE's email systems.

m. Engage in activities that violate Government laws, an Institute's contractual obligation, or any other Institute's policy or rule including but not limited to Human Resource (HR) policies and Standards of Conduct for students.

n. Comment or act on behalf of the Institute over the Internet without authenticated authorization.

o. Connect devices (such as switches, routers, hubs, computer systems, and wireless access points) that are not approved by the IAE headquarters or institutional ICT organization to the network.

p. Use without authorization any device or accessory or application that consumes a disproportionate amount of network bandwidth.

q. Respond to electronic requests (emails, instant messages, text messages, etc) that ask for generally protected information such as passwords, social security numbers or credit card numbers.

r. use ICTs for personal purposes or gains.

6.8 ICT Management Structure Set Up

The Institute has no an independent ICT Management structure (i.e. Department/Unit and a responsible committee). It is important to have a department or unit and a committee responsible for overseeing all matters pertaining to ICT issues of IAE.

Policy Statement

1. There shall be an ICT Unit responsible for all ICT issues of the IAE. The department/unit shall comprise all digital and multimedia sections of the institute like IT, Studio and Printing.
2. There shall be an independent ICT Steering Committee. The committee shall focus on;
   a) ICT strategic planning and budgeting;
   b) ICT project prioritization; and
   c) ICT project approval.

The steering committee will comprise of seven (07) members from the following proposed IAE Departments and Units:-

(i) Human Resources Management and Administration (01 person);

(ii) Adult and Continuing Education Studies Department (01 person);

(iii) Procurement Management Unit (PMU) (01 person);

(iv) IT Unit (02 persons);

(v) Research and Planning unit (01 person); and

(v) Representative from academic staff (01 person).

Principally, the Chairman unanimously elected from among members of the said committee will head the steering committee; the secretary for it ought to be the IT expert rich in ICT technical matters, skills, competence and experience.

6.9 Integration of ICT in Teaching, Learning and Administration

There are various forms of enhancing ICT integration that could be integrated in teaching and learning activities. This include; CDs, DVDs, TV, Radio, Power point presentations, You Tube Animations, Hyperlinks, E-learning, Web based technologies, Use of smart boards, videoconferencing, Social media and networks, Internet & pens etc. Integration of ICT in teaching and learning does not only deal with introduction of new hardware and software, but both trainers and the students have to adopt new roles, and change their ICT behaviours and ways of teaching and learning.

Policy Statements

1. The IAE shall ensure continuous ICT training to its staff and facilitate their full access to ICT facilities and services ensure effective and suitable integration of ICT in Teaching, learning and administration.
2. In addressing the problem of limited funds IAE should adopt freeware and open source software for teaching and learning activities.

7.0 REVISION

This policy shall be revised on a quarterly basis. Changes necessitating revision shall include changes in technology, statutory regulations and any other reasons as may be determined from time to time by the manager in

charge of ICT or the ICT steering committee. However, the office in charge of executing the policy may, from time to time, propose amendments that are necessary to enhance the objectives of this policy. Before the enactment of such amendments, the executing office shall provide opportunities to its major stakeholders to comment on the proposal. Members of the IAE community who wish to propose amendments may submit their proposed amendments to the ICT steering committee or executing office.