KAMUZU UNIVERSITY
OF HEALTH SCIENCES

Information and Communication Technology Policy

February 2024

Approved by Senate

Policy Name	ICT Policy
Policy No.	PL/C.7A.1
Effective Date	
Last Review	
Next Review	After 2 years
Council Approval Date	
Employees Subject to the Policy	Academic, Administrative and Research project employees
Responsible Office(s):	
Responsible Officer(s)	Vice Chancellor

TABLE OF CONTENTS

FOREWORD

Kamuzu University of Health Sciences (KUHeS), is a publicly funded research-intensive university that exists to advance knowledge, professional competencies, skills and innovations in health sciences through high-quality student-centred and innovative education and research that influences the global/national policy, health and development needs in an efficient, sustainable and result-oriented manner.

KUHeS is largely reliant on Information Communication and Technology (ICT) for management systems and processes using an integrated ICT approach. In this context, ICT is identified to be the foundation for maximising student, faculty, and staff productivity, ensuring efficient service delivery, enhancing teaching and learning and improving the quality of research.

Against this background, this policy document has been developed to guide the development, implementation, and effective use of ICT resources within the University. This policy will function side by side with other related published documents as the reference document on standard procedures and guidelines used within the University.

Professor Francis Moto
Chairman of Council

PREFACE

Information and Communications Technology (ICT) plays a vital role in supporting the teaching, Learning, research and administrative functions of the university.

The ICT Policy aims at guiding the development, implementation, and effective use of ICT resources within the university to enhance teaching, learning, research and innovation.

Taking advantage of the current high Technology adoption rates within the University, it is envisioned that through the policy, the university will enjoy economies of scale in a secure cyber environment, data protection, more collaboration in research, widened ICT access, modern teaching and learning technologies and research data management technologies.

However, KUHeS recognises that implementation of the Policy may be affected by the global supply chain for ICT equipment, funding limitations; and lack of adequate training opportunities for ICT personnel.

The Policy was developed in consultation with faculty members, Administrative staff and students. Implementation of this policy will require concerted team efforts of all stakeholders and especially those identified in the policy.

Professor MacPherson Mallewa
Vice Chancellor

ACKNOWLEDGEMENTS

We wish to express our gratitude and pride in the following team members who worked on the Policy:

Mr Chikumbutso Gremu, Mr Humphrey Kumwembe, Dr Arox Kamn'gona, Mr Geoffrey Chikhozo, Mr Arthur Mtegha, Mr Hubert Kanyoma, and Mr Chisomo Kaundama.

LIST OF ABBREVIATIONS AND ACRONYMS

BCP	Business Continuity Plan
DNS	Domain Name Service
DRP	Disaster Recovery Plan
ICT	Information and Communication technology
IT	Information Technology
HEI	Higher Education Institutions
KUHeS	Kamuzu University of Health Sciences
MEAL	Monitoring Evaluation Accountability and Learning
MIS	Management Information System
RA	Risk Assessment
SBU	Sub-business Unit
UPS	Uninterrupted Power Supply

DEFINITIONS

Affiliates	This means any entity supervised or controlled in connection with the university, and that exists or is organised for the benefit of the university.
Authorised personnel	Any person who has been permitted by university authority to do that work or access a restricted area
Authorised users	A person who has been given permission and rights by university authority to access University ICT services and resources.
Bandwidth	The maximum amount of data transmitted over an internet connection in a given amount of time
Business process	An activity or set of activities that accomplish a specific organisational goal.
Cybercrime	Criminal activity that either targets or uses a computer, a computer network or a networked device.
DNS	Domain Name Service (DNS) is a hierarchical naming system for computers, services, or any resource connected to the Internet or a private network.
Staff	A person who has entered into an employment relationship with the university, whether academic or professional, administrative or support staff, paid or unpaid, full-time or part-time, entire appointment or joint appointment, affiliation appointments or assistantships.
ICT service	Any form of technology that is used to transmit, process, store, create, display, share or exchange information by electronic means.

ICT resources	Any tangible or intangible asset capable of generating, transmitting, receiving, processing, or representing data in electronic form, where the asset is owned, licensed, operated, managed, or made available by, or otherwise used by, KUHeS.
ICT Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.
Personnel	A person or a group of people employed by a university responsible for various organised undertakings of the university.
Stakeholders	Entities, both persons and organisations that have an interest in and/or investment in ICT of the University and are impacted by and care about the outcomes of ICT use at the University.
Student	Any full-time or part-time graduate or undergraduate student enrolled at the University. This includes persons: a) Who have been accepted for admission to or enrolled for any course or programme offered at or in conjunction with the University or; b) Whose body of work completed while so enrolled (e.g. a research dissertation or thesis), is still under examination.
User	Staff, students and any authorised personnel who access ICT resources and services.

1. BACKGROUND AND SCOPE

ICT is central to research, curricular development and implementation, administration and management at universities. Accelerated developments in ICT have created new opportunities for Higher Education Institutions (HEI) to cope with the challenges of training increased numbers of students in this era of the knowledge society. For KUHeS to sustain the quality of its programmes, it will have to adopt and implement extensive use of ICT in its core functions which include teaching, research, consultancy and outreach. It is thus imperative for KUHeS to acquire the appropriate and adequate human resources and infrastructure to facilitate the optimal deployment of ICT services.

Thus, the formulation of this policy is to guide proper planning, development, deployment and use of ICT services at the University. It sets out the rules governing the use of ICT systems and services. The ICT systems and service shall only be used for carrying out the business of the University except where the University has expressly provided otherwise in writing and for occasional, reasonable private use. In using the University's ICT services, the conduct of any User should be such that it does not interfere with the governance and proper administration of the University, it does not interfere with the conditions necessary for teaching, learning, or research or bring the university into disrepute.

This policy must be read together with other university's rules, regulations, policies and procedures as referred to in this policy. This policy applies to all users of ICT services including staff, students, visitors and affiliates who make use of the university's ICT services. It also applies to all ICT resources and services that are owned or leased by the University, including any privately-owned hardware and software but only when the latter is used for University business.

2. RATIONALE

The University needs to continuously improve its services and increase productivity. This can be easily achieved by investing and using ICT to drive its core functions of teaching, research and outreach. However, increased dependency on ICT makes the university vulnerable to ICT-related risks. In this regard, it is evident that the university needs to develop and operationalise a comprehensive ICT Policy to direct ICT adoption and usage within the institution.

3. VISION

A world-class university and centre of excellence in health education, research, and innovation.

4. MISSION

To advance knowledge, professional competencies, skills, and innovations in health sciences through high-quality student-centered and innovative education and research that responds to and influences global/national policy, health, and development needs in an efficient, sustainable, and result-oriented manner.

5. AIM

This document provides the highest level ICT directives on management, deployment and use of ICT to ensure that ICT-related investments, operations and maintenance processes are cost-effective and efficient for the enhancement of quality research, teaching and learning, administration and management related activities. The aims of this policy are:

a. To provide equitable access to ICT services to all bonafide members of the university.
b. To strengthen and promote the use of ICT in the core functions of the University

c. To ensure that the members of the university use ICT facilities and services appropriately and responsibly.
d. To strengthen capacity to handle ICT security issues related to privacy, cyber-crime, and ethical and moral conduct.

6. OBJECTIVES

The objectives of the policy are:

a. To define mechanisms for increasing access to ICT services through shared use of ICT facilities and resources and ensuring non-discriminatory access to ICT regardless of affiliation with the university.
b. To define technologies to support the core functions of the university.
c. To provide awareness on the responsible use of ICT services to all users of ICT services.
d. To ensure adherence to security standards in the deployment of ICT resources.

7. RELATED DOCUMENTS

This ICT Policy is related to the following:

a. National ICT Policy of 2013.
b. Public Procurement and Disposal of Public Assets Act, 2016.
c. Electronic Transaction and Cyber Security Act, 2016.
d. Data Protection Act, 2024.

8. POLICY PRIORITY AREAS

8.1 ICT Governance and Management

ICT Governance is an integral part of the university governance and consists of the leadership, organisational structures and processes that ensure that the organisation's ICT sustains and extends the organisation's strategies and objectives. Effective ICT Governance provides a conducive

environment for the alignment of all ICT investments in a rationalised manner that is aligned towards enabling the university to meet its goals and objectives. This also contributes to the attainment of value for money, management of risks and effective ICT utilisation.

The University shall ensure:

a. There is an ICT steering committee responsible for reviewing and approving ICT strategies and investments, ensuring alignment with the University's objectives and goals. The committee shall be headed by the Deputy Vice Chancellor (DVC) and the Chief Information Technology Officer (CITO) who shall be secretary of the committee.
b. annual ICT audits and evaluations are conducted to assess the effectiveness and efficiency of ICT systems and processes with findings reported to Executive management for action.
c. adequate financial resources to acquire and manage ICT facilities and services.
d. ICT requisitions initiated by any other department are assessed and verified by the ICT department.
e. Enforce ICT adoption in all its functions.
f. As a way of sustaining the ICT services, each user shall be required to pay service fee recommended by the ICT steering committee and approved by the university. The payment shall be made at the beginning of the academic year.
g. All Sub-business units shall be required to pay service fees for the ICT services provided.

8.2 ICT Assets Management

Asset Management and Controlling involves activities for asset acquisition, storage, usage, maintenance and disposal. The assets include hardware, software, management information systems, data, system documentation,

and storage media, supporting assets such as computer rooms, server rooms air conditioners and Uninterrupted Power Supplies (UPS). Inappropriate use of ICT assets may expose KUHeS to risks such as loss of assets, breach of data confidentiality, malware attacks, compromised investment, compromise network systems and services and legal implications.

The University Shall:

- Ensure that ICT assets are protected physically and logically for the entire lifecycle of the asset.
- Ensuring user entitlement of ICT assets is well documented and bonded in their tenures that means all terminated users must submit all ICT assets given to them during tenure ship.
- Ensure that at the end of the project all ICT assets for project are retained by the host department.
- Ensure that ICT assets are disposed securely when no longer required.
- Ensure that any lost ICT related assets are reported immediately to the University.
- Ensure that all lost or discarded assets are recorded accordingly in the asset register
- Ensure ICT assets acquired through a third-party or vendor have appropriate service level agreement.
- Ensure that all ICT related assets are protected from power failures.
- Ensure that non-mobile hardware shall not be taken off-site without prior written authorization and documentation for future reference.
- Ensure information or software is not carried or transfer through a medium that is not allowed under its classification.
- Ensure all acquisitions of new ICT assets must be made in accordance with university policies on procurement.

- Ensure procurement of core strategic ICT assets shall be proposed by the ICT Office and procurement shall proceed only after approval.

The ICT Department shall:

- Ensure that all ICT assets are recorded and classified according to the ICT asset classification.
- There shall be an inventory system in place for ICT assets.
- Ensure all servers and other critical assets are housed in purpose-built rooms such as server room.
- Ensure only authorised personnel shall install, maintain and configure hardware and software that belongs to the university.
- Ensure periodic change of passwords to all systems at set intervals or in event of compromised passwords.
- Ensure accounts of all staff or students are deactivated when they leave the university upon receiving formal communication from the Registry.
- Ensure assets are properly maintained for continued reliability, availability and integrity.
- Ensure backup is done and tested accordingly.

8.3 ICT SECURITY GOVERNANCE AND MANAGEMENT

Effective ICT Governance practices have an impact on how securities of ICT assets are achieved at KUHeS. This includes how risks are identified, managed; how resources are allocated to implement several security measures as well as KUHeS management commitments towards achieving the notable goal of operating in a universally secured environment. Thus, the University shall:

- Ensure ICT security practices are implemented on discharging its functions while maintaining vision and mission highlighted in the strategic objectives.

- Ensure ICT security measures are adhered to in all ICT related projects.
- Allocate sufficient funds for effective ICT security and ensure capacity building on updated security issues for ICT staff.
- Ensure changes to the organization, business processes, information processing facilities and systems that affect ICT security shall be controlled.
- Ensure the entire community comply and abide by security measures, which will be put in place.
- Ensure a consistent and effective approach is applied to the management of risk and business continuation plan (BCP) implementation.

The ICT Department shall:

- Ensure regular orientation to staff and students on ICT security matters.
- Ensure local and external training of ICT staff on security matters for effectiveness and efficient security technique implementation.
- Ensure that modern security technologies are implemented.
- Ensure the review and updates of Business Continuity Plan (BCP), Disaster Recovery Plan (DRP) and Risk Assessment (RA) are done annually.

8.4 INTERNET SERVICE

The use of internet service is crucial in the daily operations at KUHeS. It is essential that users understand their role in creating efficient and cost-effective ways of communicating and obtaining information in safer environment. Improper or inappropriate use of the Internet can have an adverse effect on the university operational and can also have serious legal consequences. Therefore, The University shall:

- Ensure access to the Internet shall be available to all bonafide members of the university which include staff, students and other

authorised users and usage shall be guided by the acceptable use guidelines.

- Ensure all users including projects and SBUs within university community contribute to Internet service and other ICT services fees as a means to create sustainable robust services.
- Ensure that there is sufficient bandwidth to meet the requirements of the entire University and its campuses.
- Invest in technologies to manage Internet service to ensure that it is efficiently and effectively used.
- Ensure any planned disruption of Internet services for the purpose of upgrading the system, maintenance, etc. shall be notified to all users through official communication channels at least two working days before the anticipated disruption date.
- Ensure that robust technologies are deployed such as a firewall to control all data packets and connection requests; only explicitly permitted traffic shall be allowed, all other traffic shall be rejected; all traffic shall be logged and audited; packet filtering shall be used with rules, which keep the risk to a minimum.
- Ensure that all buildings used for academic and administrative purposes are provided with access to the university's interconnected ICT facilities through the provision of data and WIFI access points.

The following uses of the Internet system are considered unacceptable:

- Use of KUHeS Internet service to setup e-business activities not related to the University.
- Use of KUHeS's Internet service to transmit or receive obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language;
- Use of KUHeS's Internet service to access, review, upload, download, store, print, post, or distribute materials that use language or

images that are inappropriate to the work setting or disruptive to the work environment or advocate violence or discrimination toward other people or that may constitute harassment or discrimination.

- The use of the KUHeS's Internet service knowingly or recklessly post false or defamatory information about a person, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks;
- The use of the KUHeS's system to gain unauthorized access to information resources or to access another person's materials, information or files without the implied or direct permission of that person;
- To attempt to gain unauthorized access to the KUHeS system or any other system through the KUHeS Internet service, attempt to log in through another person's account, or use computer accounts, access codes or network identification other than those assigned to the user.
- If a user unintentionally accesses unacceptable materials or an unacceptable Internet site, the user shall immediately delete or report to appropriate authority for further action.
- Downloading, storage and dissemination of copyrighted materials including software and all forms of electronic data without the permission of the copyright holder or under the terms of the licenses held by the University shall be prohibited.

8.5 ELECTRONIC MAIL

The university shall ensure the availability of a secure and reliable email system and provide each student and staff with an email address under the University domain name structure.

8.6 Use of E-mail

The use of e-mail shall follow these guidelines:

a. All official communication using emails within and outside KUHeS shall require use of KUHeS official email address.

b. Where an office has a predesignated email address, all official communication of the office shall use that predesignated email to ensure business continuity.

c. Attempts to falsify identity or affiliation with the university when sending e-mail from the university's email service or any social engineering is prohibited.

d. Users are responsible for all e-mails originating from their accounts.

a. All official communication via emails within and outside KUHeS will require use of KUHeS official mail.

e. All emails sent must have a standard university signature

f. Email accounts shall be deactivated when a staff or student leaves the university.

g. KUHeS email addresses shall not be used to subscribe to non-university related websites such as betting, dating, banking, and social media sites.

8.7 Security and Confidentiality

The following security and confidentiality terms shall apply:

a. Contents of e-mail messages sent or received from the university's email service shall be treated as confidential.

b. All email messages exchanged using the university's email service belong to the university.

c. The university shall reserve the right to access the e-mail account of a user in special circumstances upon authorisation by the registrar.

d. The university shall block emails from outside hosts that send unsolicited (bulk) and malicious emails.

8.8 MANAGEMENT INFORMATION SYSTEM

The university shall automate its business processes using relevant Management Information Systems (MIS).

8.8.1 Acquisition of MIS

In addition to section 8.2, the following shall apply to the acquisition of MIS by the university.

a. The complexity of the MIS, human capacity, urgency, and cost effectiveness of acquiring the MIS shall determine whether the MIS is internally developed, outsourced or bought off-shelf.

8.8.2 Use of Management Information Systems

Use of Management Information Systems shall be guided as follows:

a. MIS shall be made available to all bonafide members of the university according to the IT principle of least privilege.
b. Only university allocated MIS accounts shall be used to conduct the university's business.
c. Staff or students are responsible for all activities originating from their accounts.
d. All MIS accounts shall be deactivated when staff or student leave the university.

8.8.3 Security and Confidentiality

The following shall apply:

a. Information from the university's MIS shall be treated as confidential.
b. The university shall deny access to all suspicious or malicious users to MIS.

c. The hosting of all MIS and data storage shall be in accordance with the University Risk Management Policy.

8.9 UNIVERSITY WEBSITE

The University's Website is an official publication of the University. Its mission is to promote the University and to provide accurate and up-to-date information in an accessible and attractive manner to the public. It is an all-encompassing site and a virtual reflection of the University community and its heritage. The university has full right for its website.

The university shall:

a. Ensure that its websites are regularly updated and have contents that conform to its mission, objectives and functions.
b. All official pages shall be maintained and regularly updated by the responsible University offices or academic units.
c. All official pages shall be regularly monitored by the Web master.
d. Graphic elements and photographs on official pages shall be governed by the university's rules and procedures on branding.
e. A system of permissions shall be adopted and used to protect the security of the university's website.
f. All websites shall include search engine optimisation.
g. All updates of content on the website shall follow laid out procedures.

Schools and departments shall:

h. Dedicate/assign staff to maintain and/or update the school's web pages. The staff shall also be responsible for checking materials for their accuracy and conformance with Web standards and for working with the Web master of the ICT Office prior to the content of the site.

8.10 DOMAIN NAME SERVICES

The use and Management of Domain Name services is critical in promoting the visibility of the University as well as improving security of systems. The University shall provide procedures and guidance for the proper use of English-like domain names instead of IP address numbers for ease of access of the University's Website.

Domain name services shall follow these steps:

a. All Domain Name Services (DNS) of the university shall be managed and monitored centrally by the ICT department.
b. According to the university's DNS standards, all services that are provided by members of the university community as part of their official functions, and as part of the mission of the institution, shall be registered within the university domain.
c. Domain names outside the university shall only be hosted with the authorisation of the Registrar.

8.11 SECURITY AND SAFETY

Security and safety measures shall not be limited to:

a. The university shall have purposely built rooms to house core ICT infrastructure which shall be secured and access shall be restricted to authorised personnel.
b. Construction and other civil works made around the university ICT infrastructure shall be done in consultation with the ICT office.
c. All unused access channels shall be deactivated or closed.
d. The use of monitoring tools, such as network analysers or similar software, shall be restricted to authorised personnel except when explicit permission is given for academic and research purposes by an authorised person.

e. Only authorised personnel are permitted to take computing equipment belonging to the university off the premises and they are responsible for its security and safety.
f. The university facilities shall be adequately protected against fire, water and any other damages caused by natural disasters.
g. Only computer devices that meet the security standards established by the university shall be connected to the university network.
h. The university network infrastructure shall be secured against all types of threats.
i. All computing equipment owned by the university or used on the university network shall have Antivirus software installed and regularly updated.
j. All data on computing equipment owned by the University must be encrypted and backed up in a university provided environment.
k. All equipment should be fully formatted and restored to factory default before transfer or disposal.
l. The disposal of computing devices shall be guided by the University Procurement and Asset Disposal Policy.
m. The university shall not use any software that has reached the end of life or is no longer supported by the owners.
n. The disposal of the software shall only take place when it is formally agreed that the system is no longer required and that its associated data files which may be archived will not require restoration at a future point in time.
o. The university shall monitor and record all activities within the university when users access the facilities, software, services and systems.
p. Use computing resources (CPU time, disk space, bandwidth) in a way that does not cause disruptions on computer systems or other users.

q. Avoid deliberate interference or unauthorised access to user accounts and data

r. Take all reasonable steps to ensure that computer equipment is protected at all times against theft and accidental or deliberate damage.

s. Treat all passwords as private and confidential.

t. Access to computing facilities shall be through a user account comprising an ID/username and password.

u. User accounts shall have access rights and privileges depending on responsibilities.

v. User accounts on all systems shall be audited regularly.

8.12ICT SECURITY SYSTEMS AND BACKUP MANAGEMENT

8.13 ICT Security

There shall be separate KUHeS ICT Security Policy. This document shall cover the following aspects of ICT:

- Networks and Internet security
- System security
- Users access, Computer access, Server room access, Remote access, Password policy
- Virus, Malware, spyware, Intrusion Detection protection

8.14 Backup and recovery Management

a. There shall be a Disaster recovery plan (DRP) and Business Continuity Plan (BCP).

b. Back-up procedures, ensuring that both data and software are regularly and securely backed-up, are essential to protect against loss of that data and software.

c. ICT team members shall ensure a daily incremental and a weekly backup to the backup servers, for the purpose of restoring a system

in the event of a system failure. In any absence of ICT member(s) then, other ICT member(s) should take responsibility for backup. In the event of a disaster IT personnel shall work hand in hand to restore user files but does not guarantee retrieval. The responsibility for backing up user files remains with the user.

8.15 ICT COMPETENCE

The adoption and use of ICT requires competence by staff and students. The university shall;

a. Ensure that all staff are competent users of ICT services, the level of competency being in line with the demands of their job functions.
b. Ensure that ICT competence programmes are offered to the university community with the objective of not only ensuring user satisfaction but also reducing the user support load on the involved ICT personnel.
c. Ensure the delivery of training focused on building skills of users that will make the users more effective in utilising ICT resources.

a. establish ICT training needs in liaison with user departments and service consumers.
b. Ensure all new staff are orientated to ICT services before using them.

c. Ensure that IT security awareness are done to the University community with the objective of equipping users with skills and knowledge on cybersecurity.

9. CHANGE MANAGEMENT

There is need to control introduction of a changes into the ICT environment by ensuring that the correct procedures are being followed.

The university shall;

- Ensure availability of procedures for managing both planned and unplanned changes
- Ensure proper testing and approval of changes before they are implemented.
- Ensure adherence to change management procedures by all requesting departments.
- ensure that all system configurations and changes are introduced in a controlled and coordinated manner.

10. GUIDING PRINCIPLES FOR IMPLEMENTATION

The implementation of this policy shall be guided by the following principles:

- Accessibility: Ensure that ICT services and resources are accessible to all members of the university, regardless of their abilities or technological proficiency.
- Security and Privacy: Prioritize the protection of data and information assets through robust cybersecurity measures and adherence to privacy regulations. Respect user privacy and ensure the confidentiality of sensitive information.
- Equity and Inclusivity: Promote equal access to ICT resources and opportunities for all stakeholders, regardless of socioeconomic status, ability, geographic location, or demographic characteristics.
- Interoperability: Foster compatibility and seamless integration between different ICT systems and platforms to enhance efficiency, collaboration, and data exchange.
- Sustainability: Embrace sustainable practices in ICT infrastructure and operations to minimize environmental impact, optimize resource utilization, and support long-term viability.
- Innovation and Adaptability: Encourage innovation and continuous improvement in ICT solutions to address evolving needs and

technological advancements. Foster a culture of experimentation and adaptability.

- Governance and Compliance: Establish clear policies, procedures, and governance structures to guide the responsible use of ICT resources and ensure compliance with relevant laws, regulations, and industry standards.
- Capacity Building and Training: Invest in training and capacity-building initiatives to empower stakeholders with the knowledge and skills needed to effectively leverage ICT resources.
- Continuous Evaluation and Improvement: Regularly monitor and evaluate the implementation of ICT policies and initiatives to identify areas for improvement and optimize outcomes over time.

11. MONITORING AND EVALUATION

The following shall guide the University:

a. An ICT steering committee shall monitor and evaluate the implementation of the ICT policy. The purpose of monitoring and evaluation is to assess progress, keep track and implement corrective measures to fulfil the objectives of the implementation plan.

b. To ensure that the ICT Policy meets its intended goals and objectives, the implementation shall be monitored and evaluated for effectiveness and responsiveness. Elements of the Monitoring Evaluation Accountability and Learning (MEAL) framework shall include objectively verifiable indicators, means of verification, milestones, and key responsibilities for each strategy.

c. Monitoring will be done continuously, evaluation shall be done periodically preferably biannually, and external ICT audit results shall feed into the university's annual report.

12. FINANCIAL IMPLICATIONS

Implementation of the Policy shall have the following financial implications:

a. Policy sensitisation workshops.
b. Licensing fees of all existing non-compliant software
c. Annual ICT Audit fees
d. Additional bandwidth costs
e. Installation of biometric access control devices and CCTV cameras