MAASAI MARA UNIVERSITY

INFORMATION COMMUNICATION TECHNOLOGY (ICT) POLICY

VERSION NUMBER:	001
REVISION NUMBER:	001
DOCUMENT STATUS:	Draft
DATE APPROVED:	
APPROVED BY:	
EFFECTIVE DATE:	
DEPARTMENT RESPONSIBLE:	ICT
DATE OF NEXT REVIEW:	

Table of Contents

1.0. Introduction

1.1 Preamble

ICT is a technical service which performs a collection of relevant tasks and functions for the management of ICT in the University. It prepares users to participate in a rapidly changing world in which work and other activities are increasingly transformed by access to varied and developing technology. The University community use ICT tools to find, explore, analyse, exchange and present information responsibly, creatively and with discrimination.

Where there is no separate ICT standards document for the University, this policy will serve, alongside other related published documents, as the reference document on ICT standards.

1.2 Statement of purpose

This policy aims to identify those ICT services that are best incorporated within the University centrally funded ICT infrastructure; define a governance and management structure for the development and implementation of ICT policies, strategies and services; and define the role of the University Information Technology Department.

Its objectives include to:

(i) provide guidance in developing a pervasive, reliable and secure ***communications infrastructure***conforming to recognized International standards supporting all services in line with the priorities of the University;

(ii) provide a framework for development and management of ICT ***network services***that shall ensure the availability, enhanced performance, security, and reduce the cost of running the ICT infrastructure;

(iii) establish information and implement ***security***requirements across the University's ICT infrastructure;

(iv) provide a framework, including guidelines, principles and procedures for the development andimplementation of ***Software Information System***projects in the University;

(v) guide the handling of ***organizational information***within the ICT department and the University as a whole by ensuring compliance with applicable statutes, regulations, and mandates for the management of information resources; and thereby establish prudent practices on ***Internet***and the ***University Intranet*** use;

(vi) uphold the integrity and image of the University through defined standards and guidelines forensuring that the content of the University's ***websites***is accurate, consistent and up-to-date;

(vii) serve as the direction pointer for the ICT department mandate in ***supporting users*****,** empowering them towards making maximum use of ICT services and resources and specifying the necessary approaches;

(viii) to guide the process of enhancing user utilization of ICT resources through ***training*****;**

(ix) outline the rules and guidelines that ensure users' PCs and other ***hardware***are in serviceable order, specifying best practices and approaches for preventing failure;

(x) to provide a paradigm for establishing the University's ***database service*** that will support groups working on systems development, production and any other groups; and,

1.3 Officer Responsible

Information Communication Technology Officer

1.4 Approving Body

The University Management

1.5 Scope of this policy

This policy applies to any person accessing/developing/implementing and/or using ICT-based information and ICT resources owned, managed, supported or operated by, or on behalf of, the University. The addresses include all University staff and students; any other organizations accessing services over University ICT resources; persons contracted to develop, repair or maintain University's ICT resources; and suppliers of outsourced ICT services.Adherence to this policy applies to all these and other relevant parties.

1.6 Definitions and interpretations

In this document, unless the context otherwise requires, the abbreviations and terms below are defined as follows:

MMU– Maasai Mara University, otherwise known as the "University"
ICT - Information and Communication Technology;
ICTD - Information and Communication Technology Department;
CMU - The Maintenance Unit of the ICTD;

1.7 Information and Communication Technology Infrastructure

The specific "infrastructure" which is the province of the policy at this time is intended to support the operational business of the University. At some future time, there may be a requirement for other dedicated infrastructure to be established for experimental or research purposes.
The scope of ICT infrastructure, defined according to the specific ICT services, depends upon tangible assets including hardware, software, communications and network services; upon support functions including Service Desk; upon appropriate training that ensures competency in the use and support of information and communication technology; upon appropriate access to relevant and helpfulInformation; and upon budget processes and policies that are matched to realistic expectations.

1.7.1 Information and communication technology core services

The Information Communication Technology Department (ICTD) will provide for the planning, developing, maintenance and the management of the University information systems, integrated databases, ICT security requirements, and ICT equipment and facilities. The composition of this set of formal ICT services will be reviewed periodically as technological options and the University requirements change.

1.7.2 Supplementary services in support of core ICT services

Effective use of the University information and communication technology services requires the provision of assistance to the clients who use the services, and to the staff who conduct the technical support for local ICT resources. It is the responsibility of local entities to ensure their staff is able to use ICT services proficiently and that their technical staff are appropriately trained and authorised by the ICTD to conduct technical support. The University will also provide ICT related training and enhancement programmes to promote awareness of ICT utilization in the University.

1.8. The Information and Communication Technology Department (ICTD)

1.8.1 Functions of the Information and Communication Technology Department (ICTD)

The focus of the Information Technology Division will be to:

1.8.1.1 Educate by training and inculcating awareness of the utilization of ICT in the University community activities leading towards the development of an advance ICT culture;
1.8.1.2 Synergize the knowledge worker and technology advancement in the electronic University environment;
1.8.1.3 Provide, support and manage the University ICT infrastructure services according to agreed Principles;
1.8.1.4 Develop detailed proposals for ICT policy, procedures and guidelines; and coordinate the ICT funding/budget planning for the University.

The ICT resources of MMU are provided to support the teaching, research, consultancy and administrative activities of the University. This policy deals with the provision of information and communication technology resources by the University and the associated responsibility of authorized users' i.e. University staff members when utilizing these resources.

The policy is based on the following principles, which must be adhered to by all those responsible for the implementation of this policy and to whom this policy applies:
1.8.1.5 The ICT resources of the University are provided to support the teaching and administrative activities of the University;
1.8.1.6 Authorized users are granted access to University resources, sensitive data and to external networks on the basis that their use of ICT resources shall be responsible, ethical and lawful at all times;

1.8.1.7 Authorized users are required to observe MMU ICT Policy, and Kenya Cyber Laws which may apply;

1.8.1.8 Data and information relating to persons and other confidential matters acquired for business purposes shall be protected;

1.8.1.9 University Business information shall be protected from unauthorized and/or accidental disclosure; and

1.8.1.10 University ICT resources must not under any circumstances be used to humiliate, intimidate, offend or vilify others on the basis of their race or gender.

Staff members are required to use the ICT resources in a responsible, ethical and lawful manner. This policy, to which all staff should adhere, identifies what is acceptable use including the personal use of ICT resources. This policy identifies the possible consequences should a breach of the policy occur.

1.9 ICT Resources

These resources cover all ICT facilities including the MMU network, all computers, computingLaboratories, all associated networks in classrooms, internet access both wired and wireless, email,Hardware, data storage, computer accounts, software (both proprietary and those developed by the University),

2.0 Access to ICT Resources

This policy prescribes the conditions under which access to MMU ICT resources is granted.

Lawful Use
The use of ICT Resources must be lawful at all times. Unlawful use will breach this policy and will be dealt with as a disciplinary offence.

Unlawful use of ICT Resources may also lead to criminal or civil legal action being taken against individual authorised users. This could result in serious consequences such as a fine, damage and/or costs being awarded against the individual or even dismissal from the University.

The University will not defend or support any authorised user who uses ICT resources for an unlawful purpose.

User Declaration Form
Users may be required to complete a Declaration form prior to authorization being granted for access to certain ICT Resources.

Third Party Access
Entities other than the ICTD may neither negotiate nor grant third parties access to the University applications, databases, communications and network infrastructure. Applications for access should be made in writing to the Principle of the University.

Domain Name Registration
All domain names for MMU projects/activities must be registered through the ICTD. This requirement must be observed in all instances. Users should note that it is the Universitythat owns and controls the site and not the person who registers the name.

Software License Restrictions
Use of licensed software is subject to terms of license agreements between the MMU and the software owner or licensor, and may be restricted in its use.

Cost of Accessing ICT Resources
The University Senate will determine the fee to be levied for accessing ICT Resources from time to time.

2.1 Personal Use of ICT Resources

2.1.1 Extent of Personal Use

An authorized user is permitted to use the ICT Resources for limited, incidental personal purposes. Personal use of the ICT Resources is permitted provided such use is lawful, does not negatively impact upon the user's work performance, hinder the work of other users, or damage the reputation, image or operations of the University. Such use must not cause noticeable additional cost to the University.

2.1.2 University Liability

The University accepts no responsibility for:

(i) Loss or damage or consequential loss or damage, arising from personal use of theUniversity ‘s ICT Resources;

(ii) Loss of data or interference with personal files arising from the University 's efforts to maintain the ICT Resources.

2.2 Internet, Email and Messaging

2.2.1 Access to the Internet

2.2.1.1 Work Purposes

Authorized users are permitted to access the Internet for work related purposes.

2.2.1.2 Personal Use

Access is also permitted for personal purposes provided such use is lawful and reasonable in terms of time and cost to the University. Examples of permitted personal use are:

(i) Communication;
(ii) Online banking;
(iii) Travel bookings;
(iv) Research;

2.2.2 Personal Web Pages

2.2.2.1 Publication of Personal Web Pages

Authorized users are permitted to publish personal web pages on computers connected to theMMU network. The content of material on personal web pages’ sites must be in accordance With:

(i) Relevant laws, particularly the Kenyan Copyright Law;
(ii) The standards and principles contained in this Policy;
(iii) The standing of the user in relation to the University and commensurate with the standardof care owed by the user to the University; and
(iv) The University vision and mission.

The University reserves the right to regularly monitor personal web page sites hosted on MMUServers, and to remove material, or request the user to remove or alter the content on their personal web page should it be inconsistent with any of the above.
Special care must be taken with web pages so as not to infringe any third party copyright in an audio or video file, music charts/lyrics, photographs or text.

2.2.2.2 Disclaimer Required on Personal Web Pages

A personal web page site must carry the MMU Personal Page Disclaimer as a standard disclaimer on every page. The disclaimer states that the web page site is not authorized by the MMU and that any opinions expressed on the pages are those of the author and not those of the University.

2.2.2.3 Responsibility for Personal Web Pages

Legal responsibility for personal pages rests with the user. The University will not defend a user named in an action arising from material published on a personal web site and will not be liable for any damages awarded against the user by a court or commission.

2.2.3 Email and Messaging

2.2.3.1 User Responsibilities

When using the email or messaging system, users must at all times:

(i) Respect the privacy and personal rights of others;
(ii) Take all reasonable steps to ensure copyright is not infringed;
(iii) Take all reasonable care not to plagiarize another person's work; or defame another person;
(iv) Not forward or otherwise copy a personal email (except with permission of the author) or an email which contains personal information or an opinion about a person whose identity is apparent (except with permission of that person);
(v) Not send forged messages, or obtain or use someone else's e-mail address or password without proper authorization;
(vi) Not send mass distribution bulk messages and/or advertising without approval of the user's Head of Department, or Administrative Unit;
(vii) Not send SPAM. The user must ensure that the recipient(s) of the intended email has/have consented to receive such email(s);
(viii) Not harass, intimidate or threaten another person or other persons:
(ix) Not send sexually explicit material, even if it is believed that the receiver will not object.

2.2.3.2 Standards Required When Using Email

The private commercial use of email and messaging is not allowed and appropriate standards of civility should be used when using email and other messaging services to communicate with other staff members, students or any other message recipients. When using the email or messaging system, users must not send:

(i) **Angry or Antagonistic Messages** – these can be perceived as bullying or threatening and may give rise to formal complaints under grievance procedures or discrimination/sexual harassment procedures;

(ii) **Offensive, Intimidating or Humiliating Emails** - University ICT Resources must not be usedto humiliate, intimidate or offend another person or other persons on the basis of their race, gender, or any other attribute prescribed under the University and Kenyan discrimination legislation.

2.3 Security of ICT Resources

2.3.1 Authorized Users' Responsibilities

Authorised Users have a responsibility at all times to:

(i) Act lawfully.
(ii) Keep all MMU ICT Resources secure and to observe the MMU ICT Security Policy.

(iii) Not compromise or attempt to compromise the security of any ICT Resource belonging to theMMU or other organizations or individuals, nor exploit or attempt to exploit any security deficiency.
(iv) Take reasonable steps to ensure physical protection including damage from improper use, food and drink spillage, electrical power management, anti-static measures, protection from theft, and sound magnetic media practices.
(v) Ensure their computers are not left unattended without first logging-out and/or securing the entrance to the work area – particularly if the computer system to which they are connected contains sensitive or valuable information.

2.3.2 Confidential Information

Authorised Users have a duty to keep confidential:

(i) All University data unless the information has been approved for external publication; and
(ii) Information provided in confidence to the University by other entities.
(iii) Each staff member is under the obligation not to disclose University business information unless authorized to do so. Breach of confidentiality through accidental or negligent disclosure may expose a user to disciplinary action.

2.3.3 University Liability

The University accepts no responsibility for:

(i) Loss or damage or consequential loss or damage, arising from the use of the University ICT Resources.
(ii) Loss of data or interference with files arising from the University efforts to maintain the ICT Resources.

2.4 Prohibited Use of ICT Resources

The following lists the prohibited acts when using the MMU ICT Resources. Any staff found to have violated this policy will be subjected to disciplinary action, and criminal offences will be reported to the relevant government authorities such as the police.

2.4.1 Advertising and Sponsorship

Paid advertisements are not permitted on any website using MMU domain name, personal website or any website, which has a substantial connection with the University (such as a website for a research programme) except with the written permission of the MMU Management.

2.4.2 No Business Activities

Authorized users are not permitted to run a business or publish a non- MMU journal/magazine(Unless prior written authorization has been obtained from the University) on MMU ICT Resources.

2.4.3 Unauthorized Access

Authorized users are expressly forbidden from gaining unauthorized access or attempting to gain unauthorized access to ICT Resources belonging to the University and other organizations.

2.4.4 Peer-to-Peer File Sharing (P2P)

Installation or use of peer to peer file sharing software such as Bit Torrente.t.c. is not permitted on the MMU network. Exceptions for legitimate teaching or research use must be approved by the University and only where no alternative technology is appropriate.

2.4.5 Pornography

Authorized users are not permitted to utilize the University's ICT Resources to access pornographic material or to create, store or distribute pornographic material of any type.

2.4.6 Gambling

Authorized users are not permitted to utilize the University's ICT Resources to gamble.

2.4.7 Computer Games

Authorized users are not permitted to utilize the University's ICT Resources to play computer games during normal office hours.

2.5 Privacy and Surveillance

2.5.1 Security and Privacy

The accounts, files and stored data including, but not limited to, email messages belonging to users at the University are normally held private and secure from intervention by other users, including the staff of the Information Communication Technology Department (ICTD).

There are others in which duly authorized ICTD staff may be required to intervene in user accounts, temporarily suspend account access or disconnect computers from the network in thecourse of maintaining the University's ICT Resources such as repairing, upgrading or restoring file servers or personal computer systems.

Users should be aware that ICTD staff may from time to time become aware of the contents of user directories and hard disk drives in the normal course of their work, and they are bound tokeep this information confidential.

2.5.2 Access to and Monitoring of Equipment

The University does not generally monitor email, files or data stored on ICTresources or traversing the University network. However, the University reserves the right to accessand monitor any computer or other electronic device connected to the MMU network. This includes equipment owned by the University and personal computing equipment (e.g. laptops or smart phones) thatare connected to the network.

Access to and monitoring of equipment is permitted for any reason, including, but notlimited to, suspected breaches by the user of his/her duties as a staff member, unlawfulactivities or breaches of University legislation and policies. Access to and monitoring of equipmentincludes, but is not limited to email, web sites, server logs and electronic files. The University maykeep a record of any monitoring or investigations.

2.6 Enforcement of this Policy

Alleged or suspected violations of the "Responsible Use of ICT Resources – MMU Staff" shouldbe reported to the Information Communication Technology Department (ICTD) of the MMU. Abuse of ICT privileges is subject to disciplinary action, which may include the loss of these privileges and other disciplinary sanctions up to and including termination of services.

A staff member who abuses the University's computing, information, and communicationsresources may also be subject to civil action and/or criminal prosecution. The University will pursuecriminal and civil prosecution of violators when appropriate. Individuals will also be responsible for anyfinancial loss to the University that results from inappropriate use of ICT resources.

2.7 RESPONSIBLE USE OF ICT RESOURCES – MMU STUDENTS

2.7.1 Purpose

The ICT resources of the MMU are provided to students, staff and authorized external users for legitimate University purposes. This will normally mean academic coursework and administration.
The purpose of this policy is to protect the essential interests of the University without inhibiting the use ofthe ICT environment, which is intended for the greater benefit of students, staff and the University generally.

2.7.2 ICT Resources

The policy governs all ICT facilities including the MMU network, all computers, computing laboratories,all associated networks in classrooms, internet access both wired and wireless, email, hardware, and data storage, computer accounts, and software (both proprietary and those developed by the University).

2.7.3 Access to the ICT Resources

Users of the ICT resources must be aware of the conditions on which access is provided. Access to theICT resources are restricted to authorised users, i.e. staff members and registered students of the MMU.

Login access to the ICT resources is granted by the Information Communication Technology Department (ICTD). The Administrator of an ICT facility may restrict access to an individual user on the grounds that the user is in breach of this policy.

This could result in serious consequences such as a fine, damages and/or costs being awarded againstthe individual or even dismissal. The University will not defend or support any student who uses ICTresources for an unlawful purpose.

2.7.4 Regulations for Responsible Use of ICT Resources:

(i) Students must abide by the terms of copyright laws, software licensing agreements, and contractsthat pertain to the University's computing, information, and communications resources. Reproduction ordistribution of copyrighted works, including, but not limited to, images, video, text, audio, or softwarewithout permission of the owner may be an infringement of the Kenyan Copyright Law.

(ii) The University's ICT resources are intended to be used to fulfill the University's vision and mission. Use of any of the University's ICT resources for personal profit or gain or for commercial purposes is strictlyprohibited.

(iii) Students must be considerate in the use of shared resources and not perform acts that are wastefulof computing resources or that unfairly monopolize resources. Examples include, but are not limited to,junk mail, chain letters, games, creating unnecessary multiple jobs or processes, obtaining unnecessaryoutput, creating unnecessary network traffic, or printing an excessive number of copies of anydocuments such as resumes, theses, and dissertations.

(iv) Students may not access, send, or store any messages and/or material that is found to be fraudulent,harassing, or in violation of any local or international law.

(v) Students are responsible for the security of their computer accounts, including the changing ofpasswords on a regular basis. Students are also responsible for all activities that originate from their accounts. Computer accounts are University property and are deactivated according to MMU policiesand procedures.

(vi) Allowing another individual to use one's computer account and/or password is strictly prohibited.

(vii) Students may not attempt to access another user's electronic communications, nor may they read,Copy, change, or delete another user's files or software without permission of the user.

(viii) Use of the campus network to gain unauthorized access to any computer account or computersystem, to attempt to bypass data protection schemes, to uncover a security loophole, or to mask their identity of a computer account or machine is prohibited.

(ix) Although the University respects the privacy of an individual's electronic communications, studentsshould be aware that files and mail messages are not guaranteed to be private or secure. Files andmessages may be viewed in the course of routine management of computing, telecommunications, andnetwork services. In the event of a security breach, suspected breach, suspected illegal activity, orsuspected

violation of University policy, files and/or mail may be accessed by authorized personnel.

(x) Students may not deliberately perform an act that will interfere with the normal operations ofcomputers, terminals, peripherals, or networks. This includes, but is not limited to, tampering with anycomponent of a local area network (LAN), Intranet, or wide area network (WAN); blockingcommunication lines; or interfering with the operational readiness of a computer.

(xi) Students may not install, run, or give to another user a program that is intended to or is likely todamage a file or computer system and/or reproduce itself on University computer systems. This includes,but is not limited to, programs known as Trojan horses, viruses, root kits, or worms.

(xii) Software and/or information that infringes upon the rights of another or that gives unauthorizedaccess to another computer account or system must not be placed on any University -owned computersystem or computer connected to the University's network.

2.8 Misuse of ICT Facilities

2.8.1 Unauthorized access to accounts

Users are expressly forbidden **unauthorized**access toAccounts, data or files on MMU ICT resources, or on ICT resources belonging to other organizations.

2.8.2 Student Computing Laboratories

Users of student computing resources are required to abideby all the rules and guidelines set by the ICTD for use of the Computing Laboratories.

2.8.3 Peer to Peer (P2P) file sharing programs

Installation or use of peer to peer file sharing programs such as Bit Torrent etc is not permitted on computers connected to the MMU network unless with express authority of ICTD.

2.8.4 Unlawful activities

Users are not permitted to use MMU ICT resources for unlawful activities e.g. infringement of copyright, defamation etc.

2.8.5 Databases, online journals, ebooks

Use of electronic resources provided by the MMU isgoverned by individual license agreements and is for non-commercial research and studypurposes only. Users are required to comply with the use restrictions set out on the specific siteor stated in the license agreement, and must not systematically download, distribute or retainsubstantial portions of information.

2.8.6 Pornography

Users are not permitted to utilize the University ICT resources to accesspornographic material or to create, store or distribute pornographic material.

2.8.7 Computer Games

Game playing is not allowed on MMU ICT resources, except as a formalcomponent of a University academic subject or through a Department, Centre or Unit sponsoredevent.

2.8.8 Assignment services

Users are not permitted to use ICT resources to sell or purchaseassignments, or to offer to write assignments or to request help with assignments.

2.8.8 No Business Activities

Users are not permitted to run a business or to publish a journalormagazine (unless authorized by the University) on MMU ICT resources.

The University reserves the right to withdraw a service or withdraw access for student ownedcomputers if there is evidence of misuse of ICT resources.

2.9 Privacy and Surveillance

The University does not generally monitor email, personal web sites, files and data stored on Universitycomputers or traversing the University network.

However, the University reserves the right to access and monitor email, web sites, server logs andelectronic files and any computer or electronic device connected to the MMU network, includingpersonally owned equipment, should it determine that there is reason to do so. Such reasons wouldinclude, but not be limited to, suspected or reported breaches of this policy, or breach of any Statutes,Regulations or policies of the University, or suspected breaches of the law.

2.10 Enforcement of this Policy

Alleged or suspected violations of the "Responsible Use of ICT Resources – MMU Students" should bereported to the UniversityManagement Board

Abuse of ICT privileges is subject to disciplinary action, which may include the loss of these privilegesand other disciplinary sanctions up to and including dismissal.

A student who abuses the University'scomputing, information, and communications resources may also be subject to civil action and/orcriminal prosecution. The University will pursue criminal and civil prosecution of violators whenappropriate. Individuals will also be responsible for any financial loss to the University that results frominappropriate use of ICT resources

3.0 Network Development and Management Policy

3.1 Introduction to network policy

The University network functions shall be broken down into the following areas:

(i) University ICT Infrastructure Development
(ii) University System
(iv) Local Area Networks (LANs)
(v) Private networks
(vi) Access to ICT facilities
(vii) Connection to and usage of ICT facilities
(viii) New or changed use of ICT equipment
(ix) Monitoring of network performance

This therefore shall require a policy that will secure the future reliability, maintainability andviability of this valuable asset.

3.2 Objectives of network policy

The objective of this policy is to establish a comprehensive and uniform Network Development and Management policy for the management of ICT infrastructure for the University.

This policy defines the arrangements and responsibilities for the development, installation, maintenance, and use and monitoring of the University's ICT networks to ensure that, these networks are sufficiently adequate, reliable and resilient to support continuous high levels of activity.

3.3 Scope of network policy

This policy applies to any person accessing or using the ICT infrastructure owned, managed, supported or operated by, or on behalf of the University. These include all University staff and students; any other organization accessing services over University ICT networks; persons contracted to repair or maintain the University's ICT networks; and suppliers of network services.

3.4 General network policy

3.4.1 The Network

The University will develop and support a University-wide ICT network as a basic infrastructure service for the facilitation of sharing electronic information and resources by all members of the University. This includes all staff and students of the University, and other persons engaged in legitimate University functions as may be determined from time to time.

3.4.2 Universal availability

(a) The University network will be designed and implemented in such a way as to serve those located at the University and, to a lesser extent, those located elsewhere.

(b) The ultimate goal is that every room in the University in which research, teaching or support activities take place should be connected. And every member of the University should have capability to access the University ICT infrastructure.

(c) The University network will form part of the general fabric or infrastructure of the University.

(d) There will be one coherent network supporting access to all general information services provided to the University members.

3.4.3 Reliability

(a) High levels of availability, reliability and maintenance will be major objectives in the construction and operation of the University ICT network.

(b) The design and construction of the University network will take into account emerging technologies and standards wherever possible.

3.5 ICT Infrastructure Development Policy

3.5.1 Development plan

The ICT will prepare a rolling network development plan, advising on appropriate developments aimed at ensuring the adequacy of the University's ICT infrastructure in future. This plan will take account of the University's strategic plan; usage and demand patterns; technological change; security; management and cost implications.

3.5.2 ICT network provision in new and refurbished buildings

(a) Network provision for new and refurbished buildings shall be made in accordance with the

(a) Specification published from time-to-time by the ICT department.

(b) Where the Network requirements are of specialized nature the Officer in Charge concerned shall seek further guidance from the network manager.

(c) All new buildings to be erected in the University shall incorporate an appropriate structured data wiring system to allow connection to the University network.

3.6 University System

3.6.1 Definition

The network will consist of several parts: systems, a collection of inter-building connections; "Campus LANs,"University "Dial-up" service; and a number of "Server Farms." The UniversityNetwork system will comprise an inter-building cabling system, together with one or more "Gateway" interfaces at each building or in the path to each building which will connect the System to the network(s) within each building.

3.6.2 Structure of University System

(a) The University Network System shall connect, singly or severally, to buildings, not to individual departments or units.
(b) The planning, installation, maintenance and support of the University
(a) Network System shall be under the control of the ICT Department.
(b) Connection to the University Network System shall be approved by the ICT Manager ICT department.
(c) The ICT department shall adhere to and maintain copies of all relevant networking standards, and keep abreast of national and international developments in these standards.
(d) The University Network System at any particular point of time will be aimed at facilitating the traffic flow between connected buildings or networks.

3.7 University LANs

3.7.1 Definition

The respective schools/departments will take responsibility for the LANs, namely, the necessary wiring and related equipment within existing buildings to allow connection to the LAN gateways.

3.7.2 Structure of LANs

(a) Wherever feasible, the network(s) within each building shall be arranged so that there is a point of connection to the University Network System. In cases where it is not possible to establish a single connection, multiple building gateways may be installed.
(b) Network protocols used on building networks and communicating through the gateway must use approved configuration parameters including approved network identifiers.
(c) Building networks connecting to the University network shall meet overall University network security and management requirements.
(d) In cases where there are constraints to connecting any building to the University Network System, consultations and subsequent approvals by the ICT Manager shall be made to allow for alternative configurations.

3.8 Dial-up Access

3.8.1 Definition

Authenticated access through telephone dial-up access via designated Packet Switched Telephone Network (PSTN) telephone numbers to network services provided for staff and students.

3.8.2 Structure of dial-up access

(a) Network protocols used on the service shall use approved configuration parameters includingapproved network identifiers.

(b) Dial-up links connecting to the University network shall meet overall the University network security and management requirements.
(c) The dial-up links shall provide authenticated off-campus access to designated information systems and services available on the network using normal individual usernames and passwords.

4.0 Private networks

4.1 Definition

Departments or units may install, at their own expense, networks independent of the University Network System. Provided that the installation shall not interfere with the University network. And provided the installation shall adhere to the University policies and standards for installing and implementing such networks.

4.2 Structure of private networks

(a) Private departmental networks may extend between buildings.
(b) The ICT department may provide links for these networks but any extra expense incurred above the University Network System requirements shall be charged to the Department.
(c) The ICT department shall provide Campus Gateways for private departmental networks where the private network caters for all the building occupants.

4.3 Access to ICT facilities

4.3.1 Communications rooms, cabinets and ICT network equipment

(a) All communications rooms and cabinets shall be locked at all times.
(b) Entry to communications rooms and cabinets, and interference with ICT network equipment is strictly prohibited.
(c) Other than in an emergency, access to communications rooms, cabinets and ICT network equipment shall be restricted to designated members of staff of the ICT department. Any necessary access must have prior written consent of the ICT Manager.

4.3.2 Access in an emergency

(a) In the event of a fire or other emergency, security staff and/or staff of the Estates Department and/or the emergency services may enter these areas, without permission, to deal with the incident.
(b) Where ICT network equipment is housed in accommodation used for another purpose, the
(a) Arrangements for access by another user of that accommodation shall require the prior writtenconsent of the ICT Manager. This consent shall specifically exclude access by the other user toany communications cabinets or ICT network equipment located in the shared accommodation.

4.3.3 Installation of cabling

All installations and changes of electrical power cabling in facilities housing ICT equipment shall be approved and managed by the Administration in consultation with the ICT Manager in writing.

4.3.4 Installation of equipment

The specification of any equipment to be installed in communications rooms and cabinets and the installation of such equipment, shall require the prior written consent of the ICT Manager.

4.3.5 Network equipment

(a) Only designated members of the staff of ICT department are authorized to install and maintain active network equipment including hubs, switches and routers connected to the University's ICT networks.

(b) Where the ICT Manager of the ICT department agrees that academic staff or the ICT department technical staff may install and maintain hubs and switches within local staff or student networks, such permission will in every case specifically exclude the point at which these hubs and switches connect to the University's network infrastructure.

4.4 Connection to and Usage of ICT facilities

4.4.1 Connecting to the ICT network

(a) All connections to the University's ICT networks must conform to the protocols defined by the ICT department and with the requirements that apply to Internet Protocol (IP) addresses.
(b) Only designated members of staff of the ICT department, or other staff authorized specifically by the ICT Manager, may make initial connections of desktop services equipment to the ICT network.
(c) Computer workstations connected to the ICT network will not be set up to offer services to other users, for example, to act as servers, unless the prior written consent of the ICT Manager has been obtained. Such consent will normally exclude all external access.

4.4.2 Domain name services

All Domain Name Services (DNS) activities hosted within the University shall be managed and monitored centrally, for the whole University , by the ICT department.

4.4.3 Electronic mail

Electronic mail or email shall be received and stored on central servers managed by the ICT department from where it can be accessed or downloaded by individual account holders.

4.4.4 Suspension and/or termination of access to ICT networks

4.4.4.1 University Employees

(a) A staff's access to the University's ICT networks will be revoked automatically:

a. at the end of his or her employment or research contract;
b. at the request of his or her Dean of Faculty/Head of Resource Centre/Head of Department or

(b) School or Head of Unit;
a. Where he or she has breached these regulations.

(c) The University reserves the right to revoke staff's access to the University's ICT networks where the user is suspended pursuant to a disciplinary investigation.

(d) The Administration Registrar will establish mechanisms whereby changes in employment status are communicated immediately to the ICT Manager so that these employees' computing and e-mail accounts can be suspended or deleted as appropriate.

4.4.4.2Students leaving the University

(e) The Academic Registrar will notify the ICT department, by means of the regular student data transfer, of the names of students leaving the University so that such students' computing, e-mail, printing and lending accounts can be deleted.

4.4.4.3Procedures on Restriction of Use

(f) Appropriate procedures shall apply in restricting usage after a formal complaint has been lodged or a breach of policy or rule has been reported or detected.

(g) Any breach of ICT policies shall be reported or communicated in writing to the ICT Manager

(h) Upon receipt of any such complaint, ICT manager shall classify the complaint as "serious" or "non-serious." A "non-serious" complaint shall be defined as a breach of policy which does not subject the University to a cost nor any risk.

(d) When a complaint is classified as "non-serious, ICT Manager, is authorized to impose any one of the following penalties:
i. Suspension of the account for a minimum period of four weeks
ii. Permanent disabling of the account

(e) When a complaint is classified as "serious," ICT Manager shall refer the complaint to the ICT Committee for appropriate action. The possible penalties may be any one or a combination of the following:

i. Notification of the suspension will be communicated to the relevant Dean and/or Head of
ii. Department or Section;
iii. Suspension of the account shall be for a minimum period of four weeks. Formal approval of the relevant Dean and/or Head of Department or Head of Section and a signed undertaking to abide by the Rules of Use shall be required before reinstatement of the account.
iv. Permanent disabling of the account shall be taken, where the severity of the offence warrantssuch action.
v. Accounts may be reinstated before the end of the suspension period where either the student or staff presents information to the ICT Manager, which indicates that he or she was not involved

vi. in the transgression of the Rules of Use, or the Dean and/or the Head of Department or Head ofSection requests the account be reinstated for course related work only (e.g. completion of anassignment). In this case the student or staff is required to sign an undertaking to abide by theRules of use.

vii. A system administrator within MMU can make a recommendation to disable an account to theICT Manager. The ICT Manager shall review the request and if there is considered to be, on thebalance of probability, a transgression of the MMU ICT Rules of Use, the account shall besuspended.

viii. An account may also be suspended, if a request has been made to the ICT Manager, from asystems administrator of another system, with a reasonable and accepted case for suspension.

ix. Users should note that suspension of access to ICT facilities also includes access to the terminal server password access, and as such dial-up modem access will be disabled where a user account is suspended.

4.4.4.4 Appeals

Students or staffs whose access has been suspended shall have the right to appeal in writing to the ICT Committee.

4.4.5 Internet Protocol (IP) addresses

(a) All equipment connected to the ICT department networks shall be assigned unique IP addresses.

(b) The IP addresses assigned to equipment shall be recorded visibly on the Networking File.

(c) The Communications and Networks Manager, ICT department shall plan and allocate Blocks of IP addresses to different network segments and notify the relevant Officer in charge.

(d) The Officer in Charge, after distribution of the allocated IP Block shall notify the Communications and Networks Manager who shall in turn update the IP address Networking File.

(e) The Communications and Networks Manager shall maintain a central record of IP addresses and may remove inactive IP addresses after six months.

4.4.6 Inventory control

As part of their audit responsibilities, Officer in Charge shall be required to record in their local equipment inventory records the IP address assigned to each item of equipment for which they are responsible, together with the location of such equipment.

4.4.7 Connection of privately owned computers to the University Network

Although members of staff and students may apply for an IP address, using the procedures in this Policy, to enable them to connect such computers or workstations to the University network, permission shall be given only where the Communications and Networks Manager, ICT department, is satisfied that the computer workstation meets the specification determined by the ICT and that it poses no risk to the University network.

4.4.8 Additional or changed equipment

(a) The ICT Manager shall be advised in advance and at the earliest opportunity, of any plan to add items of desktop services equipment to or to replace or to relocate desktop equipment that are connected or that may require connection to theUniversity's ICT network.

(b) The ICT Manager shall assess the likely impact on the University's ICT networks of the proposed change. The ICT Manager shall give approval for the proposed change only where appropriate adjustments can be made to accommodate any effects on network traffic that this change may cause.

4.4.9 External data communications

(a) All external data communications shall be channeled through the University's approved links.

(b) No external network connections shall be made without the prior written consent of the ICT Manager.

(c) The installation and use of leased or private links on premises owned, managed or occupied by the University shall require the prior written consent of the Estates Manager.

(d) The use of modems, leased or other means of access to other networks on equipment located on premises owned, managed or occupied by the University that are linked to the ICT network infrastructure, is prohibited, unless a proposal and justification for such connection has been authorized in writing by the ICT Manager.

4.5 Web cache provision

(a) The ICT department shall be responsible for provision and management of University web cache facilities for incoming web traffic.

(b) All web access shall be set up to ensure use of the University's web cache facility for incoming web traffic under the ICT Internet Usage Policy.

4.6 Web filtering

The ICT Manager, ICT department shall be responsible for the implementation of appropriate filtering facilities for web based and non-web Internet traffic, including MP3 traffic and other high bandwidth intensive services that may not have direct educational or research value, where and when necessary in conformity with the ICT Policy and relevant ICT Guidelines that promise efficient and high availability of Internet services to the majority of users.

4.7 New or changed use of ICT equipment

(a) The ICT Manager ICT department shall be advised in advance of any plan that involves a new use, a change of use or addition to the University's ICT networks that might impact on the performance or security of the network.

(b) The ICT Manager, ICT Department shall assess the likely impact of the proposed use and will advise on the consequential impact upon the performance of the University's ICT network. Such changes shall be effected after approval by the ICT Manager.

4.8 Monitoring of network performance

The Network Manager, ICT department, shall monitor and document ICT network performance and usage and shall maintain regular monthly reports.

4.9 ICTD Equipment Maintenance Policy

4.9.1 Definition of Terms

4.9.2 ICT equipment

means desktop computers, laptops, servers, monitors, printers, audio-visual (AV) equipment, software and network equipment, but excludes IT consumables such as printer cartridges.

4.9.3 Hardware

Is the computer equipment - the CPU, the monitor, the keyboard, the mouse, the external speakers, the scanner, the printer, e.t.c. The physical, touchable parts of a computer system.

4.9.3.1 Brand name system

A brand name computer (both hardware and software) is based on a particular company's architecture aimed at providing a unique service to its customers.

4.9.3.2Clone or semi brand system

A clone is a computer system (both hardware and software) based on another company's system and designed to be compatible with it.

4.9.4 Introduction

ICTD is responsible for maintenance of all system, hardware and network.
Computer Maintenance is done on a quarterly, weekly, monthly, daily and yearly basis.
A schedule is prepared to show all the maintenance that will be done on all the IT equipment within the university.
This schedule will be sent to the users to inform them on when the maintenance will be carried out on their respective computers. If a change is required to be made in the dates, this will be communicated to ICTD by the user/ department.

4.9.5 Policy objective

This policy document outlines the rules and guidelines that ensure that users' PCs and related hardware are in serviceable order. It specifies best practices and approaches in ICT equipment maintenance.

4.9.6 Scope

This policy applies to Information and Communication Technology (ICT) equipment, whether hardware or software, purchased by the University.

This policy applies to any person accessing or using the ICT infrastructure owned, managed, supported or operated by, or on behalf of, the University, including all University staff and students; and any other organization accessing University ICT services including persons contracted to repair or maintain the University's ICT equipment and suppliers of such equipment.

It describes the procedural steps that are to be followed by the maintenance staff in the process of providing repair support.

4.9.7 Policies

4.9.7.1 Hardware Maintenance

The ICTD shall maintain and support the supportable hardwarecategories that are commonly required by users for use in their offices, computer rooms, laboratories and lecture halls to perform their daily responsibilities. Users shall follow the ICT procurement policy for hardware in order to guarantee support by ICT.

4.9.7.2 Personal owned computer equipment/peripherals

The ICTD shall not take responsibility for the replacement, repair or upgrade of personal owned equipment/peripherals.

4.9.7.3 Maintenance schedule

(a) Users shall resolve identified/basic problems as the first level of maintenance and support.
(b) At the second level, the ICT shall then offer support to the users on issues they cannot resolve.
(c) At the third level ICT Manager shall handle issues escalated from various schools/departments.
(d) The fourth and final level should enable the senior procurement officer to work in liaison with vendors, suppliers and hardware manufacturers to repair and/or replace faulty equipment.
(e) The senior procurement officer shall be charged with the responsibility of enforcing any maintenance contracts, agreements and warranties.

4.9.7.4 Tools and equipment

Every departments/schools shall have a stock of support tools that is continually being stocked. In addition, a stock of shared tools shall be maintained centrally at the ICT main office.

4.9.7.5 Preventive maintenance

A schedule for maintenance shall be drawn, recognizing every piece of hardware. Preventive maintenance shall be carried out according to the recommendations of the

manufacturer of the hardware, in terms of frequency and method of maintenance. However, where justified by the case, service shall be provided on the basis of request.

4.9.7.6 Obsolescence of hardware

ICT hardware shall be declared obsolete according to the recommendations of the manufacturer. The hardware maintenance team shall periodically conduct maintenance to identify, retire and replace the hardware categorized as at "end-of-life."

4.9.7.7 Outsourced Service Agreement for Critical Equipment

Equipment not supportableby ICT shall as far as possible be placed on maintenance contracts.

4.9.8 Computer Systems and Peripherals

In the case of computer systems, departments that purchase the equipment shall be responsible for the following with the aid of ICT Department:

(a) Installation and administration of the system.
(b) Adequate operating environment (floor space, climate control, ventilation, and backup power supply) for the system.
(c) Routine maintenance and upgrade of the system.
(d) All expenses incurred during repair, maintenance, and upgrade.
(e) Full compliance with the University's Procurement and Disposal Policy/Act.
(f) Full compliance with the University's security policy, including installation and regular update of the anti-virus software.

Supplies for spares to support such systems and peripherals shall be the responsibility of the department.

4.9.9 Maintenance workshops

Every schools/department shall have a designated repair facility. This facility shall take the form of a room reserved for the purpose of conducting all hardware repair and maintenance activities. The ICT staff in the University shall have custody of such facility.

4.9.10 Warranty guidelines

Maintenance staff at the ICT shall facilitate the repair and maintenance of equipment under warranty.
They shall keep accurate records of the warranty of the individual items of equipment and use such information when needed to operationalize the warranty and/or guarantee for the equipment.

Note: Equipment not supportable by ICT include; Generators, Digital Line Printers, Air Conditioners and high end UPS.

5.0 ICT Training Policy

5.1 Introduction

ThisICT training policy will help the University to be clear about what IT is needed for the agency to work efficiently and the skills needed to use it effectively.
A variety of services are developed and produced by the ICT in response to the business requirements of the University. Upon production, these services are distributed (or made available) to users. Thereafter, continuous and carefully tailored training support is necessary in order for the users to fully exploit them.

5.2 Objective

The objective of this policy is providing one-on-one support to assist both academic and non-academic staff in improving their ICT skills.

5.3 Scope

(a) This policy applies to any person accessing or using the ICT infrastructure owned, managed, supported or operated by, or on behalf of, the University, including all University staff and students; and any other organization accessing University ICT services including persons contracted to repair or maintain the University's ICT equipment and suppliers of such equipment.
(b) This policy specifies the general approach to the training of all University staff and students; and any other organization accessing University ICT services, as the primary users of ICT services.
(c) It addresses the training content and methodology for ICT users.

5.4 Policy Statements

5.4.1 ICT Literacy

It shall be mandatory for all University staff to be literate users of ICT services, the level of literacy being in line with the demands of their job functions. Training shall therefore focus on building skills in users making them effective in exploiting provided ICT resources.

5.4.2 Mode of Training

(a) External ICT training shall be organized by the ICTD in response to need as may be assessed from time to time when training is not possible within the University.
(b) Internal ICT user training targeting the university community shall be scheduled on a continuous basis and shall be conducted in the University at the ICT Department.

5.4.3 Trainees

(a) The ICT staff shall jointly with user departments nominate trainees for external ICT training when the need for such training arises.

5.4.4 Training Resources

The ICT Department shall in liaison with either the Project Manager or the producer of the relevant services identify the appropriate trainers for the training. These shall be as demanded by the needs of the scheduled training.

The ICT Department jointly with the user departments shall provide necessary resources to facilitate the training.

5.4.5 Training needs and Curriculum Development

Project Managers and service developers shall establish ICT training needs in liaison with user departments and service consumers. In cases where the ICT is not well placed to train in a given area, the ICT shall identify and recommend appropriate training and work out the cost for competent trainers.

(a) The ICT shall develop curricula for all training including development of source material. To this end, the ICTDshall:-

i. Recommend curriculum for all external training
ii. Where possible provide training materials on-line via the University website.
iii. Where possible conduct on-line assessment tests and examinations.

(b) Where external training is sourced, the ICT Department shall jointly with the external training agent, customize the content to meet the training needs of the users.

5.4.6 Acknowledgement of training

The ICTD shall issue certificates on successful completion of training and examination.

6.0 User Support Policy

6.1 Definition of terms

ICT user support services
ICT services directed at ICT users to enable users to effectively exploit ICT technologies, products and services available at the University. These shall mean all activities, carried out by the support personnel involving setup, creation, procurement and acquisition, installation and deployment, repair and training on ICT technologies, and products and services, with the aim of assisting users to maximize expected utility and benefit

Hardware
All University-owned computer and peripheral equipment (such as printers, scanners, CD-ROMS (Read only memory compact discs), network cards and multimedia equipment).Excluded from such equipment would be equipment that is already under an existing service contract, warranty, nonstandard ICT equipment for which only advisory information shall be provided.

Hardware support: Attending to problems associated with hardware categories as listed under the support policy.

Software support
Attending to problems associated with software categories as listed under the support policy.

MIS support
It is thesupport for corporate systems used by the University.

ICT project
Any ICT work or undertaking that happens only once, and has a clear beginning and end, and is intended to create or deploy a unique ICT technology, product, knowledge or service.

Tools and equipment
The stock of shared tools maintained both centrally at ICTD.

6.2Introduction

The ICT acquires, develops and produces a variety of ICT technologies, products and services in response to the academic business and related requirements of the University. Upon production, these require are distributed (or made available) to users. Thereafter, continuous and carefully tailored support is necessary in order for the users to fully exploit them. A policy guideline is necessary for this support.

6.3Policy objective

(a) A guideline for the ICT User Support Service for enabling *bona fide* University ICT users to productively exploit provided University ICT resources.
(b) Specific Services include: General User Support Service; PC and User Peripheral Service; Hardware Maintenance Service; Network Support Service; ICT Staff Professional Training Service; ICT User Training Service; Operationalization of ICT Projects.

6.4 Scope

This guideline shall steer the activities of producers and consumers of ICT technologies, products and services across the University.

6.5 Policy Statements

University ICT projects and services
The ICT Manager shall ensure that ICT Support services to assist University ICT Users with technical and logistical support in the implementation.

Advocacy
The ICT Centre through User Support services shall provide users with consultancy services on any ICT matter; it shall provide technical representation in all ICT related meetings and committees; it shall communicate relevant User Support information to users, and provide them with liaison interface (or escalation point) to the greater ICT.

Support Coverage
(a) Support departments/schools shall be designated by University and to some extent by function. These shall be as detailed in the schedule of support coverage in the standards document.
(b) The ICT Support function shall provide qualified support personnel at each University. ICT
(a) Support personnel shall be deployed in accordance with the assessed support load per support department/school. The load shall be proportional to the extent to which ICTs are in use, determined mainly by the expansion of the University network and number of users there off.

Procurement Support
The ICT User Support function shall assist users in deriving the technical requirements and specifications of all ICT acquisitions and purchases. Other acquisitions and purchases must meet the minimum specifications as outlined in the ICT procurement policy for all hardware, software, services and consumables in order to guarantee support by ICT under the categories outlined above. The ICT User Support function shall verify all ICT acquisitions and purchases.

Infrastructure support

The ICT User Support function shall assist users in carrying out surveys, design, requirements, specifications, and preparation of BQs, material acquisition and supervision of implementation of all ICT infrastructures at the University.

Hardware Support

(a) The User shall be responsible for daily care and basic routine maintenance of ICT hardware under their care. ***(Refer to ICT Maintenance equipment Policy)***

(b) On a second level, the ICT Support Function shall support the hardware categories that are commonly required by users in their offices, computer rooms, laboratories and lecture theatres to perform their job responsibilities. These shall include servers, desktop computers, laptop computers, printers, scanners, digital cameras, liquid crystal display (LCD) projectors, *PDAs* (palm or pocket PC), UPS, network access hardware, among others.

Software and MIS Support

(a) ICT Support shall support software categories that are commonly required by users for use in their offices, computer rooms, laboratories and lecture halls to perform their job responsibilities.

(b) Acquisitions shall meet the minimum specifications as outlined in the ICT procurement and ICT MIS development policies for software and MIS in order to guarantee support by IC**T**. The supported categories shall include PC Operating Systems, PC Applications and Client Software, Security and Antivirus, PC backup support, among others.

ICT services support

(a) The ICT shall support ICT services that are commonly required by users in their offices, computer rooms, laboratories and lecture halls to adequately perform their job responsibilities.

(b) Acquisitions shall meet the minimum specifications as outlined in the ICT procurement policy for software in order to guarantee support by ICT.

Departmental Support

(a) The ICT shall act as the second level support to the existing Computer Laboratory Attendant or Administrator for University Basic Operation Units (BOU) with ICT personnel. The ICTC shall be available to consult or to help with significant problems.

(b) The ICT centre shall not be available to provide basic and routine cleaning and simple troubleshooting for machines except where such computer laboratories are directly owned by the ICT.

Network devices

The ICT shall own core network active devices such as switches, routers, bridges, gateways and related equipment including enclosures, and shall be responsible for the following:

(a) Creating and maintaining adequate operating environment (floor space, climate control, ventilation, backup power supply) for the equipment.

(b) Routine maintenance and upgrade of the equipment.

(c) Advising on all expenses incurred during repair, maintenance, and upgrade.

Printing facilities

A Basic Operation Unit in the University shall implement a centralized printing facility at which most print jobs shall be processed. This shall be equipped with at least one print device of appropriate specification that shall be administered from a print server. The facility shall also be equipped with at least one photocopier.

Escalation of support requests

Where necessary the ICT Support Function shall escalate user support requests to appropriate ICT sections and to other University functional units.

Support resources

(a) The BOU shall provide Office and workshop space, furniture, and basic office amenities.

Tools and equipment

Every department/schools shall have a stock of support tools consisting of items as listed on the schedule dedicated for the support work within. In addition, a stock of shared tools shall be maintained centrally at ICT.

Dress and gear

Support personnel shall be supplied with protective and safety clothing and gear suitable for the tasks involved in the support activities. These shall include items such as overalls, dustcoats, dust masks, safety gloves and the management of the ICTC from time to time may determine other items.

Logistical Resources

(a) Towards realizing the set support standards such as turn-around time and low down time, ICT shall ensure availability of logistical resources for transport to ensure rapid movement between support sites, and, communications to ensure contact between support personnel.

(b) Transportation*:* There shall be sufficient transport services available for the support function.

(c) Communication*:* Support personnel shall be equipped with appropriate communication equipment to maintain effective contact with one another in the course of duty.

Enforcement

(a) The enforcement of this policy shall be the responsibility of the ICT Department. This shall be ensured through strict adherence to the ICT standards.

(b) Violations will be addressed by established University and National Legal Mechanisms.

(c) Where required and applicable, an ICT Committee shall provide oversights, insights and guidance in case of any violation.