INFORMATION & COMMUNICATION TECHNOLOGY POLICY

DATE OF APPROVAL BY COUNCIL: .....

COUNCIL CHAIRPERSON'S SIGNATURE: .....

Dr. Frank Bunnya Sebbowa

Table of Contents

PREAMBLE

The purpose of this document is to describe the ICT policies and procedures that will guide on how ICT shall be used to achieve the goals and objectives of Muteesa I Royal University within all the teaching, learning, research and administrative units. The document highlights on the implementation, usage, maintenance of ICT as well as optimal distribution of ICT resources (hardware, software, data and human resources). This ICT policy seeks to enumerate the rules necessary to ensure the existence of the highest levels of consistency, control and harmonious interaction with ICT.

The Policies will be reviewed periodically to ensure they remain relevant and aligned to the University's goals and objectives.

POLICY STATEMENT

Muteesa I Royal University considers Information and Communication Technologies as tools that aid in the manipulation, analysis, storage, and transfer of information.

MRU ensures that all its primary and secondary stakeholders are provided with effective and efficient ICT facilities.

The following constitute rationale for user access suspension and/ or termination to University computing resources:

a) End of student or staff employment tenure
b) Request from University Council, University Management, Heads of Department and/ or University Human Resource Department
c) Occurrence of any of the unacceptable usage restrictions.

GENERAL SCOPE

The MRU ICT policy applies to all University's Departments / Units and Faculties and contains the following policies, their objectives and strategies:

i. Acceptable ICT Facilities Usage policy
ii. Electronic Mail and Social Media Policy.
iii. Data Backup and Restoration Policy.
iv. Cyber Security Policy.
v. ICT Procurement and Software Acquisition Policy.
vi. Server Room and Computer Laboratory Policy.
vii. ICT Maintenance Policy.

1. Acceptable ICT Facilities Usage Policy.

This policy ensures that all MRU's ICT facilities (hardware, software, network, services and systems) are used by staff, students and guests in an appropriate, responsible, and ethical manner. This policy also applies to the use of privately owned computers or notebooks connected to the University network.

1.1. Objectives.

i. To discourage the irresponsible and inappropriate use of hardware and network resources, which use may result in the degradation of service.
ii. To protect and preserve the privacy of individual users and the public at large.
iii. To ensure the security, reliability and privacy of MRU's system and network infrastructure.
iv. To propagate the image and reputation of MRU as a reliable and responsible University.

1.2. Strategies.

i. MRU reserves the right to monitor and record all activities related to University activities using ICT facilities.
ii. The MRU community as a whole must be warned that they must not use any ICT facility in any illegal, immoral or otherwise unauthorized manner.

iii. The Department, Management Information Systems must disseminate information to sensitize users on irresponsible and inappropriate acts in the use of ICT facilities, which use may result in the degradation of service.
iv. The Department, Management Information Systems must ensure availability of measures to protect and preserve the privacy of individual users and the public at large and must promote safety of users and network infrastructure.
v. Users shall not share individual access passphrases
vi. Users shall not use any pirated software on University computing devices.
vii. Users shall not use any unauthorized peer to peer software
viii. Users shall not get involved in action that contravenes the Computer Misuse Act (2011) or the Anti-pornography Act (2014).
ix. Users shall not get involved in action that violates the rights of any person or entity's legally registered copyright and/ or Intellectual Property.
x. Users shall not introduce any malicious software onto any University computing device or network.
xi. Users shall not get involved in any action that disrupts the normal functioning of any university computing device or network
xii. Users shall not get involved in password cracking, software spying, privilege escalation, unauthorized network port scanning and network reconnaissance, network and/or software penetration
xiii. Users shall not use University computing devices and/ or network to disrupt an external system or network.
xiv. Users shall not use University computing devices and/ or network to send out any spam
xv. Users shall not use University computing devices and/ or network for any gambling activity.
xvi. Users shall not use University computing devices and/ or network for any personal commercial purposes.

2. Electronic Mail and Social Media Policy.

This policy ensures that the provided electronic communication infrastructure that includes computing resources, network connectivity, and software tools for electronic communication (e-mail) and electronic social interaction (Facebook, Twitter, WhatsApp) amongst its subscribers and communities is a privilege, not a right and should be treated as such by all users.

2.1. Objectives.

i. To ensure proper use of MRU's electronic communication infrastructure and electronic social interaction by all stakeholders as well as enhance personal and professional reputations online.

ii. To support teaching, learning, research and administrative functions of MRU.

2.2. Strategies.

i. All e-mail communications (and associated attachments, objects, graphics, videos) transmitted or received by MRU network are subject to the provision of this policy, regardless of whether the communication was sent or received on a private or MRU owned computer.

ii. The Department, Management Information Systems is responsible for creating email addresses for new members of the MRU community. This also includes access rights e.g. passwords.

iii. The Department, Management Information Systems is responsible for disabling email addresses for ex-members of the MRU community and members that misuse or illegally use email communications without prior notice.

iv. The mailbox owner is responsible and liable for all messages sent from their e-mail accounts and ultimately responsible for all activity performed under their account.

v. The mailbox owner must keep his password secret e.g. by not disclosing it out to another person, frequently changing it, not writing passwords down or using any other processes that facilitate automatic log-on.
vi. The mailbox owner must use only e-mail account that he/she is authorized to use. This should be used for legal, moral and authorized activities, e.g. by not committing a crime using his/her email account.
vii. The mailbox owner is expected to regularly carry out some activities to manage email accounts and documents, For example: Reading all the new e-mail messages at least once in every 1 or 3 days and replying as soon as possible, Not letting messages build up in the Inbox and Outbox and deleting messages as soon they are no longer needed and logging out of the email account before exiting the application.
viii. The Mailbox owners are expected to adopt practices that increase privacy and confidentiality of their email communications. For example: They should be aware that e-mail messages may be sent to incorrect e-mail addresses, it may be possible for other people to read or change messages that you send by forwarding them to others, new e-mail will be prevented from coming into the mailbox once the mailbox has reached the maximum allowable storage space.
ix. Only the University official social media sites will be allowed to make use of University trademarks and symbols
x. Only authorized personnel by the University shall be allowed to make postings on the university official social media sites.
xi. All information shared across the university social media sites should not make reference to any biased statements on matters such as politics, religion, race, gender, statements that contain obscenities or vulgarities.
xii. All staff social media activity shall respect the Laws relating to copyright and other intellectual property rights, defamation, privacy, and other applicable laws.

xiii. All staff social media activity shall not portray colleagues in an unfavorable light in respect of matters including, but not limited to, religion, gender, race, nationality or disability.

xiv. All staff social media activity shall maintain adherence to the overall University Confidentiality agreements and information disclosure and shall not make reference to any sensitive staff or student information

3. Data Backup and Restoration Policy.

This policy ensures that copies of critical data are retained and available in case of disaster, software or hardware failures. This policy applies to only staff of the University who create, process and store data and information using the ICT resources.

3.1. Objectives.

i. To define the backup and restoration of data and information associated with the University operations.

ii. To restore copies of University critical data in case of disaster, software or hardware failures.

3.2. Strategies.

i. The Department, Management Information Systems is responsible for performing daily back up for the entire critical corporate database for the entire University.

ii. The Department, Management Information Systems is responsible for keeping back up disks in an offsite locked place only known to the Vice Chancellor.

iii. The Department, Management Information Systems is responsible for clearly marking all back up disks with a name and creation date for easy identification.

iv. The Department, Management Information Systems is responsible for providing the necessary storage and backup support to staff.

v. The Department, Management Information Systems is responsible for periodically testing the backup disks to ensure they are recoverable.

vi. The Individual users shall be responsible for backing up their own data which is on their own desktops and notebook computers.

4. Cyber Security Policy.

This policy ensures that the University digital infrastructure and information assets are protected against any compromise or attack that may affect its confidentiality, integrity and/ or availability.

4.1. Objectives.

i. To ensure the protection, resiliency and stability of all University ICT infrastructure, the information held there within and services against any cyber threats.

4.2. Strategies.

i. The Department, Management Information Systems is responsible for installing anti-virus software to ensure that all networked computer servers, computers and notebooks used by the University users are protected against virus infections.

ii. The Department, Management Information Systems is responsible for maintaining an updated ICT risk register in line with the following from the National Information Security Framework.

iii. The Department, Management Information Systems is responsible for implementing periodic systems and infrastructure audit based on the Plan, Do, Check, Act (PDCA) cycle.

iv. The Department, Management Information Systems is responsible for maintaining updated and documented secure configurations baselines for all hardware and software.
v. The Department, Management Information Systems is responsible for developing and implementing a patch management plan.
vi. The Department, Management Information Systems is responsible for implementing network filtering to protect the network against malware related threats.
vii. The Department, Management Information Systems must ensure controlled and audited usage of ICT administrative privileges.
viii. The Department, Management Information Systems must ensure that all ICT equipment are installed with the appropriate active malware protection that is continuously updated.
ix. The Department, Management Information Systems is responsible for developing and maintaining a handover mechanism for ICT equipment and information during end of staff employment contracts aligned to the University Human Resource Policy.
x. The Department, Management Information Systems is responsible for securing access to all the university ICT resources and enforce acceptable usage of the same by the deployment of security standards, technologies and best practices.
xi. Users shall ensure compliance to the cyber security policy and report any cyber security incident to the Manager, Management Information Systems.

5. ICT Procurement and Software Acquisition Policy.

This policy ensures that all ICT equipment and services are in conformity with the overall University procurement of goods and services standard as aligned to the Public Procurement and Disposal of Public Assets Act (PPDA). It also ensures that software that the University adopts provides the service as expected.

5.1. Objectives.

i. To guide the procurement and acquisition of all University ICT equipment and services towards ensuring standardization of all ICT related assets, transparency, timely delivery, quality assurance, value for money as well as compatibility with existing infrastructure and services.

5.2. Strategies.

i. Muteesa I Royal University Procurement and Disposal Unit shall manage all procurement or disposal activities within the Universities in line with the PPDA.
ii. User departments shall ensure conformity with the University Procurement Policy as implemented by the procurement and Disposal Unit.
iii. User departments shall ensure conformity with approved technical guidelines and standards by the University ICT unit in the procurement of any ICT equipment, software or service.
iv. The University ICT unit is responsible for providing technical assistance in the development of specifications for any ICT equipment, software or service.
v. The University ICT unit is responsible for providing technical assistance in the identification of user department ICT needs.

vi. The University ICT unit shall ensure and verify that supplied ICT equipment, software or services comply with the approved ICT specifications, standards and guidelines.
vii. The University ICT unit shall ensure that installation and configuration of any procured ICT equipment, software or service complies with the approved ICT specifications, standards and guidelines.
viii. The University ICT unit shall maintain an updated inventory of all ICT hardware and software indicating the life cycle.
ix. The University ICT unit shall provide support for bulk procurement of commonly used ICT equipment and software as per University need.
x. The University shall define the life cycle for each category of procured ICT equipment to determine the replacement cycle.
xi. Disposal of retired ICT equipment shall comply with the PPDA.
xii. User department shall adhere to the rules and regulations set aside for the proper usage of the ICT equipment, software or services.
xiii. User department shall report to the Head of the relevant unit, any bugs or malfunctions observed on the ICT equipment or software.
xiv. User department shall use the software legally e.g. ensure against copyright infringements on software.
xv. User department shall install copies of personally owned or free software on University machines, and then report such software to the Department, Management Information Systems for recording in the software inventory.

6. Server Room and Computer Laboratory Policy.

This policy ensures that the University server room and computer laboratories are secure and well facilitated with all the necessary ICT equipment.

6.1. Objectives.

i. To manage the use of server room and computer lab and to maintain their security.

6.2. Strategies.

i. The University ICT unit shall ensure that Server Room facilities are located in secure strong locations away from human or vehicle traffic.
ii. The University ICT unit shall ensure that Server Room facilities are protected against power fluctuations and supported by alternate power supply.
iii. The University ICT unit shall ensure that Server Room facilities are protected against physical intrusion and exposure to water, dust and fire.
iv. The University Lab Attendant shall ensure that all Computer Lab facilities are compliant to ICT approved baseline setup and configurations.
v. The University Lab Attendant shall ensure that all Computer Lab facilities are routinely checked for unauthorized connections.
vi. The University Lab Attendant shall ensure that all Computer Lab facilities are accessed only by authorized students and/ or researchers.
vii. The University Lab Attendant shall ensure that all Computer Lab facilities are locked down to prevent physical theft of any component.
viii. The University Lab Attendant shall ensure that all Computer Lab facilities are protected against exposure to water leakages, fire and or dust.
ix. The University Lab Attendant shall ensure that all Computer Lab facilities are labelled according to approved ICT nomenclature.
x. The University Lab Attendant shall ensure that all Computer Lab facilities are professionally serviced and maintained.

xi. The Students shall not bring food or drink into the computer lab.

xii. The Students shall not smoke in the computer lab.

xiii. The Students shall report problems promptly to the University Lab Attendant.

xiv. The Students shall not alter the configuration of hardware or software. This has been set up to cater for a wide range of users.

xv. The Students shall leave each piece of equipment set up as found. Do not remove any items from the computer lab.

xvi. The Students shall follow any directions posted in the venue by the staff in the management of ICT.

xvii. The Students shall not use computer resources to do non-University related activities and cause network traffic.

xviii. The Students shall keep the computer lab clean and free of hazards.

xix. The Students shall not place software or other files on University computers where these may lead to damage or legal charges (destructive programs such as viruses, pirated software, etc.).

xx. The Students shall not use the facilities to make unauthorized copies of copyright, licensed or patented material.

xxi. The Students shall not use the facilities to defraud or to create false or misleading information.

xxii. The Students shall not attempt to access any areas of any systems for which authority has not been granted.

xxiii. The Students shall not attempt to monitor or read another user's files or communications.

xxiv. The Students shall report unethical activity to University Lab Attendant.

7. ICT Maintenance Policy.

This policy ensures that the usage of ICT devices within the University has a well-planned maintenance plan so as to ensure their safety and proper usage.

7.1. Objectives.

i. To ensure that all ICT equipment are regularly maintained to ensure that all systems run smoothly with less downtime.

7.2. Strategies.

i. The University ICT unit shall from time to time define and disseminate updated ICT equipment maintenance guidelines to all Units and Faculties.
ii. The University ICT unit shall act as the central point of contact for all University ICT equipment maintenance.
iii. The University ICT unit shall provide technical support in the development and implementation of service and maintenance schedules for all University ICT equipment.
iv. The University ICT unit shall undertake a periodic assessment in all Units and Faculties to ensure compliance with the set maintenance guidelines.
v. All Units and Faculties within the University shall maintain records of all ICT equipment they acquire including records of manufacturer equipment warranty.
vi. All Units and Faculties within the University shall liaise with the unit responsible for ICT in developing service and maintenance schedules on an annual basis for all ICT equipment.
vii. All Units and Faculties within the University shall maintain good documentation describing the service and maintenance history for all ICT equipment.
viii. All Units and Faculties within the University shall ensure all ICT equipment are placed within adequate operating environments.

ix. All Units and Faculties within the University shall ensure all replacements or upgrades of any ICT equipment is undertaken with clearance from the University ICT unit.

POLICY VIOLATIONS

1. The procedure that follows after a violation of this policy is reported or noticed is that:

   i. The Head of the Department, Management of Information Systems and Quality assurance will set up a team to investigate the allegation or suspicion. If it is a student being investigated, the Dean of the Faculty he / she belongs to must be part of this team. If it is a member of staff being investigated, the Deputy Vice Chancellor must be part of this team.
   ii. The Head of the Department, Management of Information Systems and Quality assurance will temporarily suspend or block access to an account, prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of University or other computing ICT resources or to protect the University from liability.
   iii. After investigations are complete, the findings will be forwarded to the disciplinary committee, which will decide whether the suspect is guilty or not, and which will determine the disciplinary action to be taken.

2. Users who violate this policy may be denied access to University ICT resources and may be subject to other penalties and disciplinary action, both within and outside the University. Violations will normally be handled through the University disciplinary procedures applicable to the relevant user.

POLICY DEVELOPMENT PLAYERS

The ICT policy development team is composed of the Manager, Management Information Systems, ICT System Administrator, ICT Technician, Web Master and Quality Assurance Manager.

POLICY IMPLEMENTATION AND EVALUATION

The implementation and evaluation of the of the MRU's ICT policy is performed by the Department, Management Information Systems and Quality Assurance in consultation with the University Management.

POLICY MONITORING AND REVIEW

The monitoring and reviewing progress of the MRU's ICT policy is performed by the Department, Management Information Systems and Quality Assurance in consultation with the University Management. The Policy will be reviewed periodically to ensure it remains relevant and aligned to the goals of the University.