MUAST

MARONDERA UNIVERSITY
OF AGRICULTURAL SCIENCES AND TECHNOLOGY

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY

POLICY NO. ICTP/15/25

ICT 15/25

MUAST

MARONDERA UNIVERSITY
OF AGRICULTURAL SCIENCES AND TECHNOLOGY

TITLE	MARONDERA UNIVERSITY OF AGRICULTURAL SCIENCES AND TECHNOLOGY INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY
STANDARD OPERATING PROCEDURES NUMBER	
COMPILED BY	INFORMATION AND COMMUNICATION TECHNOLOGY (ICT)
APPROVED BY	COUNCIL
DATE	

EXECUTIVE SUMMARY

Marondera University of Agricultural Sciences and Technology (MUAST) ICT services are primarily meant to support the essential functions of teaching, research, outreach/community service, and administration of the University. The users of these services are essentially those who are engaged in these university activities. To ensure that the Information and Communication Technology (ICT) resources are used effectively and lawfully, it is essential to precisely define the target users and the terms and conditions under which the ICT resources are used. The MUAST ICTS department henceforth sets out this ICT policy document as a guiding principle that ensure compliance, acceptable and secure use of information communication technology by the MUAST community to succeed in achieving its mission and objectives. The document contains Information Communication Technology (ICT) policies, and also outlines responsibilities of those who use computing and networking facilities at the university. Users of these services are required to read, understand and agree to abide by and be subject to the terms and conditions contained in this manual (which may be amended from time to time) and all other applicable university policies. A deliberate breach of this policy will lead to disciplinary measures being taken against the offender through existing staff or student disciplinary procedures which may include being denied access to ICT resources. This document does not attempt to anticipate every situation that may arise and does not relieve anyone of their obligation to use common sense and good judgment. The ICT Policy document will be effective from the date of approval.

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1
1.0 INTRODUCTION 3
2.0 OBJECTIVES 3
3.0 DEFINITION OF TERMS 3
4.0 ICT GENERAL USER POLICY 4
5.0 ICT EQUIPMENT 6
6.0 ICT SERVICES 7
7.0 SECURITY AND SAFETY 11
8.0 USER SUPPORT AND TRAINING 13
9.0 AMENDMENTS 15
ACKNOWLEDGEMENT FORM 16

1.0 INTRODUCTION

The Information Communication Technology (ICT) department is a support services department responsible for provision and maintenance of ICT resources to support the day-to-day operations of the institution. The department's mandate is to provide guidance in the development, use and maintenance of a reliable, secure and cost-effective ICT infrastructure that conforms to recognized standards for acceptable and appropriate use of all ICT resources installed and configured for use at MUAST. The ICT Policy document seeks to ensure legal compliance by the university community so as to prevent and/or protect from attack, abuse, damage, loss or theft of data, ICT resources and users within MUAST.

Ensure that MUAST adheres to anti-corruption circulars, policies, and measures as directed to the attention of the University by other agencies of the State. The policy shall also serve as a deterrent to corruption since it hinders the growth, prosperity, and inclusive development of the country. The policy therefore prompts good governance buttressed by transparency, accountability, integrity, and the rule of law. This policy also acknowledges the responsibility to lead, by example, in the fight against corruption and to render services ethically.

2.0 OBJECTIVES

The objectives of this policy are to:

2.1 provide guidelines for the conditions of acceptable and appropriate use of ICT resources stalled and configured for use at MUAST;
2.2 provide standards for users in the management and use of ICT resources;
2.3 prevent/protect from attack, abuse, damage, loss or theft of data and ICT resources within MUAST;
2.4 ensure the confidentiality, integrity and availability of data and ICT resources within MUAST;
2.5 encourage and create awareness so as to enable users to understand their own responsibility for protecting ICT resources of MUAST; and
2.6 prevent bad publicity and putting the name of the university into disrepute.

3.0 DEFINITION OF TERMS

In this document:

3.1 **ICT** refers to any existing or upcoming technology that is used for the generation, processing and distribution of data and information using computer hardware and software, network, telecommunications, and digital electronics.
3.2 **Users** refers to:
  3.2.1 academic and administrative staff (permanent as well as contractual employees),
  3.2.2 currently enrolled postgraduate and undergraduate students, and other affiliated individuals or organizations authorized by the Vice Chancellor or his/her designate.

3.3 ICT Office refers to the Information Communication Technology department of MUAST.

3.4 System Administrator refers to a person who is authorized as being responsible for the configuration, maintenance, and operation of MUAST ICT infrastructure.

3.5 Software refers to the collection of programs installed on University servers or computers as well as on network devices such as switches and routers.

3.6 Software Acquisition refers to the procurement of software that will be used for solving specific problems or improving the day-to-day activities such as administration, student management, teaching-learning, research, etc. of the University.

3.7 E-learning refers to ICT-enabled transfer of skills and knowledge and may comprise all forms of electronically supported learning and teaching.

3.8 For this policy, Artificial Intelligence (AI) refers to systems capable of performing tasks that typically require human intelligence, including but not limited to machine learning, natural language processing, and robotics.

4.0 ICT GENERAL USER POLICY

The University's ICT resources exist and are maintained to facilitate and support MUAST's activities, that is teaching, research and administrative functions. All users shall be lawful, efficient, economical and ethical in their use of ICT resources. Under no circumstances may anyone use MUAST ICT resources in ways that are illegal, threaten the university status, or interfere with reasonable use by other members of the university community. The inclusion of AI in our ICT policy aims to ensure the ethical and responsible use of AI technologies while fostering innovation and maintaining compliance with relevant laws and regulations.

4.1 Eligibility

Access to ICT resources is provided to employees of the university, administration, staff, and enrolled students consistent with their responsibilities. Other individuals, upon submission of a request, may be granted access to some or all of MUAST ICT resources by the ICT Director or the Vice Chancellor of the university. The terms of access will be stated at the time access is granted.

4.2 Access to MUAST ICT Resources

Access to MUAST ICT resources will be controlled through individual user accounts and passwords. Each user of the MUAST ICT e-resources system is required to read and sign a copy of the ICT Policy before receiving an email access account and password.

4.2.1 User Accounts

The standard naming convention for staff member accounts for access to electronic systems comprises the first initial of the first name, followed by the middle initial, and the full last name. If duplicates occur, the middle initial is generally taken out to resolve ambiguity.

For students, the student registration number will be used in place of names. It is the responsibility of the employee to protect the confidentiality of their account and password information.

4.2.2 Internet Access

All offices, laboratories, and classrooms on campus are wired for access to the Internet. Network connections, wiring, equipment, or jacks may not be altered or extended beyond the location of their intended use. If departments request additional network jacks or if network connections need to be moved to different locations, the department should request this service through the ICT department. Internet Protocol (IP) addresses are provided by the ICT department and computers connected to the network may not be used as servers for private enterprises, commercial activity, or personal profit. Also computers connected to the network may not be used to provide access to the Internet for anyone not formally affiliated with the University.

Where a personal computer on MUAST network is to be used as a server for file sharing or other services, the owner of the computer must register it with ICT department in order to obtain a static IP address. However, if bandwidth or other problems occur, the ICT department reserves the right to discontinue access to the machine.

4.2.3 Access Termination

ICT reserves the rights to disconnect any network port whose activity causes an adverse effect on the network or on any other user. Network connections may also be revoked in the case of malicious or inappropriate computing activity on the network. The ICT department reserves the right to restrict access to the network during expansion, or for diagnostic and maintenance services. Every effort will be made to provide advance notification and schedule such disruptions during times of minimum impact and traffic.

4.2.4 Computer Laboratories

Users of computer labs should abide to the rules of the lab as instructed by the ICT lab technician. Users shall not be allowed to bring in and or consume food and drinks in the labs. Doing so may result in the termination of access to use any of the computer labs at MUAST. All users should provide identification to access the labs. When leaving the labs, users will be subject to search by the security officers and or the ICT member in charge. Individual computers shall be registered with the security officer and or lab technicians before they can be taken into the computer lab.

5.0 ICT EQUIPMENT

ICT equipment refers to computers, computer software, peripherals, printers, scanners, hubs, switches, routers, servers, networking cables, etc. This ICT Policy document provide procedures and guidance for the proper acquisition, installation, and maintenance of all MUAST ICT equipment, both hardware and software.

5.1 University Equipment

Users shall take all reasonable steps to ensure that computer equipment in their possession or under their control are protected at all times against theft and accidental or deliberate damage. Each employee is responsible for taking reasonable safety precautions in regard to the University owned ICT equipment. Employees will be held responsible for damage to such equipment arising out of their negligence or intentional misconduct.

5.1.1 Acquisition

All purchases of new ICT equipment or new components for existing ICT systems must be made in accordance with University policies through a structured evaluation process. Such purchase requests shall be based upon a User Requirements Specification document and shall take account of long-term organizational business needs. Any ICT equipment coming to the University through purchase or grant shall be given clearance by the ICT department to ensure usefulness, compatibility, ease of maintenance and economic viability of the equipment. Upon purchase of ICT equipment, backward and forward compatibility shall be investigated by the ICT Office.

5.1.2 Installation

Only personnel authorized by the ICT department shall install and configure ICT equipment that belongs to the University after consulting the installation guide and manual of the respective equipment. All new ICT hardware and software installations shall be planned formally and notified to all interested parties ahead of the proposed installation date. All configured and installed ICT equipment must be fully and comprehensively tested and formally accepted by users before being deployed.

5.1.3 Inventory Management

The ICT department shall keep a full inventory of all computer equipment and software in use throughout the University. Computer hardware and software audits shall be carried out periodically to track unauthorized copies of software and unauthorized changes to hardware and software configurations. End users are not supposed to move ICT related equipment from the position that they were deployed by the ICT department. All computer equipment movements

shall be done by a member of the ICT department. Only authorized personnel are permitted to take computerized equipment belonging to the University off the premises and they will be responsible for its security and safety.

5.1.4 Repair And Maintenance

All ICT equipment owned, leased or licensed by the University shall be supported by appropriate maintenance facilities by qualified technicians through the ICT department. Adequate resources shall be made available for a regular maintenance of MUAST ICT equipment. The ICT department shall put in place an elaborate programme of refurbishment and replacement of obsolete and outdated computer equipment. Machines that are replaced are returned to ICT department who will then reassigns the machines or sells them through the campus salvage process. If a hardware problem is suspected the user should call the ICT Helpdesk during normal business hours for assistance. If hardware service is indicated, arrangements will be made with the ICT technician and the user is supposed to login the complaint to the technician's log book. Deliberate or accidental damage to the university's ICT property shall be reported to the ICT department as soon as it is noticed The ICT department also provides repair for personally owned computers. Such computers will be repaired at a cost rate established by ICT department. There is a minimum charge for examining the equipment if repair is not needed. Equipment must be delivered to the ICT office during regular business hours. Payment for the repairs must be made by cash, before the equipment is picked up. Payment is done at the Bursary cash office, in the ICT projects generation fund account.

6.0 ICT SERVICES

ICT services refer to all Information Communication Technology facilities and services provided by MUAST's ICT department including, but not limited to, email system, web-based applications, integrated systems, internet and wireless communications.

6.1 Internet

Internet use on MUAST is for the purpose of conducting the university's business. However, limited personal use of the Internet is acceptable, provided such personal use does not interfere in any way with the University business use of the facilities and does not jeopardize the operation of the university's computing facilities.

6.1.1 Usage Policy

For proper usage of Internet services, users are required to firmly follow this Internet Usage policy.

i. University facilities may under no circumstances be used to obtain, view, or reach any pornographic, or otherwise immoral or unethical Internet sites.

ii. The creation, dissemination, storage and display of obscene or pornographic materials, indecent images of children, hate literature, defamatory materials or materials likely to cause offence to others is prohibited.

iii. The use of the University's Internet services to engage in hacking other sites, and accessing unauthorized information within and outside the University is not allowed.

iv. The 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 MUAST is prohibited.

Any planned disruption of Internet services for the purpose of upgrading the system or maintenance shall be notified to all users by e-mail at least two working days before the anticipated disruption date.

6.2 Electronic Mail (E-Mail)

The University shall provide e-mail services on its network to support its academic and administrative functions to all users. E-mail use on MUAST network is for the purpose of conducting university business. However, the University allows limited personal use of the e-mail system, provided that such personal use does not interfere in any way with the University's business use of the system and does not jeopardize the operation of the University's computing or e-mail facilities. In order to enable users to share information, improve communication, exchange ideas and improve productivity, the University encourages the use of e-mail. For proper usage of the e-mail service, users are required to firmly follow this e-mail policy.

6.3 Usage Policy

E-mail service shall be made available to all users upon request to the ICT department. Academic and administrative units may request e-mail accounts for visiting scholars and other guests who are in some way affiliated with the University, specifying the duration of the account. Only responsible personal use is permitted provided that it is not likely to cause loss to the University, is not for personal financial gain, does not contravene any of the University's policies and guidelines, is not detrimental to the University's image, and does

not interfere with work. Users are responsible for all e-mail originating from their user accounts.

The following are strictly prohibited:

6.3.1 Sending of pornography or pornographic jokes or stories.

6.3.2 Use of the e-mail system to engage in communications that are in violation of MUAST policy including but not limited to transmission of abusive, obscene, offensive or harassing messages, or messages that disclose personal information without authorization.

6.3.3 Attempts to falsify identity, or to pretend having a different affiliation with MUAST when sending e-mail from a University computer as well as conduct of any social engineering.

6.3.4 Use of MUAST e-mail service for junk or unsolicited bulk mail, and chain letters.

6.3.5 Using the identity and password of someone else for access or otherwise attempting to evade, disable, or "crack" password or other security provisions.

Any planned disruption of e-mail service for the purpose of upgrading the system or maintenance shall be notified to all users by e-mail at least two working days before the anticipated disruption date.

6.4 Security And Confidentiality

The contents of e-mail messages sent or received are generally intended to be confidential. A user's e-mail received/sent through MUAST is considered private. The University shall not read the content of an e-mail unless there is a court order. The University reserves the right to refuse e-mail from outside hosts that send unsolicited (bulk), mass or commercial messages, or messages that are considered as threats, or messages that appear to contain viruses, and to filter, refuse or discard such messages.

6.5 Closure of an E-Mail Account

An email account of a staff member that is dismissed, resigned, or deceased shall be closed/deactivated as soon as the event is notified to the ICT department by the appropriate University unit. A retired staff shall be able to use his/her university e-mail account. A user's account of a student dismissed for non-academic reasons shall be deactivated with immediate effect upon notification to the ICT department by the Registrar. A user's account of a student that is academically dismissed or has graduated shall remain active for a maximum of one year when the event is notified to the ICT department by the Registrar. Users' accounts that are closed for any reason shall be archived for a minimum of one year. Anyone who does not comply with the rules and regulations of MUAST's e-mail use may have his/her account closed/deactivated with immediate effect.

6.6 **Web Publishing**

The MUAST Website is an official publication of the university aimed at supporting its academic and administrative functions. The purpose of the website is to promote the University and provide accurate and up-to-date information in an accessible and attractive manner to audiences inside and outside of the University. It is expected to represent MUAST's mission and its character, just as other MUAST's publications strive to do.

6.7 **University Webpages**

All official pages of the university shall be built using template pages supplied through the Web administrator and shall be regularly updated by the responsible University offices or academic units. Each webpage within the MUAST's Website shall be readily identifiable as a part of its site by the use of the University logo or logotype, a specific palette of colors and specific typefaces. All official pages shall be regularly monitored by the Web administrator to ascertain that the material is current. Those with outdated materials will be notified to update their page or remove the outdated material.

6.8 **Web Authoring**

The Web administrator and his/her designated person(s) from user departments are responsible for the university website. The designated person(s) will be working with the Web administrator and help build, add to, maintain and/or update the Webpages. He/she shall also be responsible for checking the accuracy of materials and ensure that they are well-written, concise, and free of spelling and grammatical errors prior to their publication on the site. All Web authoring tools shall be in compliance with the Content Management System used by the University.

6.9 **Website Security**

A system of permissions shall be adopted and used to protect the security of the University's Website. Those with full permissions to administer the Webpages will be limited and will be designated by the ICT department as necessary to maintain Webpages. Permissions to author on the site will be given by the Web administrator. All employees with full or limited permissions to the University Website are responsible for taking all reasonable precautions to protect both the public and developmental Website areas from vandalism, hacking and accidental alteration. This includes not sharing computer account information or passwords with others and carefully monitoring access to personal computers in shared work areas.

6.10 **Domain Name Services**

Domain Name Service (DNS) is a hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. All domain name services of the University shall be managed and monitored

centrally by the ICT department. Domain names outside muast.ac.zw shall not be allowed on the University network.

6.11 E-Learning

It is in MUAST's interest to promote e-learning and to integrate ICT in teaching and learning to enhance staff effectiveness thereby improving the quality of graduates and also provide greater access to university education. The ICT department shall establish the appropriate e-learning platforms responsive to academic needs. The ICT department shall ensure that all students and academic staff are trained on a continuous basis to equip them with the requisite skills to fully exploit the university's e-learning systems.

6.12 Social Media

The term "social media" refers to a set of online tools that supports social interaction among users. These include but not limited to WhatsApp, Facebook, Twitter, Flicker, YouTube, Instagram etc. MUAST currently maintains social media presence on Facebook, Twitter and YouTube. User should note that all MUAST social media sites represent the university and as such information published on these sites should conform to all applicable MUAST policies. There shall be no posting of biased statements on matters such as politics, religion, race, gender, sexual orientation, nationality or disability. There shall be no posting of statements that contain obscenities or vulgarities or that can cause anxiety and panic.

7.0 SECURITY AND SAFETY

Security and safety is about protection of ICT infrastructure, data and the user community against attacks from internal or external sources. Deliberate attempts to degrade the performance of the University network or to deprive access to resources by authorized personnel or access to any ICT facilities is prohibited. The University shall give high priority to preventing threats from being materialized and therefore users are required to adhere to this security and safety policy.

7.1 Security

The University shall identify and isolate secured areas such as server rooms from physical contact or access. LAN and WAN equipment such as switches, hubs, routers, and firewalls shall be kept in secured rooms. In addition, the equipment shall be stored in lockable communication cabinets. Access to secured areas shall be restricted to authorized personnel only. During non-working hours, secure areas shall be protected against intrusion by appropriate access control, locks, and surveillance systems or by security personnel. Breach of security includes, but not limited to, the following:

i. creating or propagating viruses,
ii. hacking, password grabbing,
iii. disc scavenging,
iv. social engineering, etc.

7.1.1 Firewall

A firewall shall be used on MUAST network to control all data packets and connection requests. A packet filtering firewall shall be used with rules, which keep the risk to a minimum. Only explicitly permitted traffic will be allowed through the firewall and all other traffic shall be rejected. All traffic passing through the firewall must be capable of being logged and audited.

7.1.2 Antivirus Software

All computers used on the MUAST network must have a standard antivirus software installed. The ICT department shall install standard antivirus software to ensure that all servers, workstations, and laptops owned by MUAST are protected against virus infection. The University requires all existing and incoming students to install antivirus software on their personal computers by the end of the second week of classes each semester. Failure to do so can result in the loss of connectivity to the MUAST network until an antivirus software is installed. Avast antivirus software is provided free to all students. Other antivirus products may be substituted as long as they are updated on a regular basis. Users shall call for assistance immediately if a virus incident is noticed and cannot be cleaned by the user. Deliberate actions that might reduce the effectiveness of any antivirus or other ICT security management precautions installed by authorized University personnel is prohibited.

7.1.3 Monitoring Software

The use of monitoring tools, such as network analyzers or similar software, shall be restricted to authorized ICT personnel who are responsible for network management and security purpose only except when explicit permission is given for academic and research purposes by an authorized person. Purposefully scanning internal or external machines in an attempt to discover or exploit known computer software or network vulnerabilities is prohibited.

7.2 Safety

The University, through the ICT department, shall set out procedures and operation manual with the consideration of preventing anticipated threats that may damage physical devices. ICT infrastructure shall be adequately protected against fire, water and physical damage.

7.2.1 Server Rooms

Computer server rooms shall contain an adequate air conditioning system in order to provide a stable operating environment and to reduce the risk of system crashes due to component failure.

7.2.2 Workstations

Users shall log out of their workstations when they leave their workstation for any length of time. All users of workstations, personal computers or laptops shall ensure that their screens are locked when not being used. All unused workstations shall be switched off outside working hours.

7.2.3 Electrical Safety

Power feeds to servers shall be connected through uninterrupted power supply (UPS) and surge protector equipment to allow the smooth shutdown and protection of computer systems in case of power failure. All switches, routers, firewalls and critical network equipment shall be fitted with UPS. All UPS equipment shall be tested periodically.

8.0 USER SUPPORT AND TRAINING

A variety of services or systems may be developed and produced 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 and support is necessary in order for the users to fully exploit them. The objective of this user support and training policy is, therefore, to outline a guiding reference when providing user support and when planning for, organizing, and conducting ICT training.

8.1 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. Computer literacy programmers shall be offered to the University community with the objective of not only ensuring user satisfaction but also reducing the user support load on the ICT department. Training shall focus on building skills of users making them effective in utilizing ICT resources.

8.2 Training

The ICT department shall establish ICT training needs in liaison with user departments and service consumers. ICT training that targets the University community shall be scheduled on a continuous basis. The ICT department jointly with the user departments, shall provide the necessary resources to facilitate the training. External ICT training shall be organized by the ICT department in response to the needs as may be assessed from time to time when training is not possible within the University. Where training is outsourced, the ICT department shall jointly with the external training agency, customize the content to meet the training needs of the users.

8.3 User Support

User support shall be provided in the form of informed help on academic and administrative computing and information to all users. Computing services shall continue to be provided with strong user support to ensure integrated access to information services. All information system and hardware faults shall be reported promptly and recorded in a fault register. Technical audits shall be undertaken at least every three years by the ICT department to determine the performance of computers and recommendations shall be made for replacement or otherwise.

8.4 Artificial Intelligence (AI)

8.4.1 Purpose

The inclusion of AI in our ICT policy aims to ensure the ethical and responsible use of AI technologies while fostering innovation and maintaining compliance with relevant laws and regulations.

8.4.2 Scope Of AI

AI technologies may be utilized in data analysis, automated decision-making processes, and customer service operations, among other applications.

8.4.3 Ethical Use of AI

All AI systems must be designed and implemented in a manner that is transparent, fair, and accountable, with efforts made to eliminate bias and discrimination.

8.4.4 Data Privacy

AI systems must comply with all applicable data protection laws, ensuring that data collection and usage are conducted with user consent and that personal data is handled securely.

8.4.5 Monitoring

Regular audits and evaluations of AI systems will be conducted to ensure compliance with this policy and to assess their effectiveness.

8.4.6 Training

All employees will receive training on the ethical implications of AI technologies and their responsibilities in using these systems

8.4.7 Reporting

Any concerns regarding the use of AI technologies should be reported to the designated compliance officer.

8.4.8 Interpretation and Implementation of AI:

The university will embrace AI to support its processes and activities.

8.4.9 Review:

Clauses about AI will be reviewed annually and updated as necessary to reflect changes in technology, legislation, and ethical standards

9.0 AMENDMENTS

This ICT policy shall, in general, be reviewed at least every two years. However, the ICT department may, from time to time, propose amendments that are necessary to enhance the objectives of this policy. Before the enactment of such amendments, the ICT department shall provide opportunities to major stakeholders to comment on the proposal. Members of the University community who wish to propose amendments may submit their proposed amendments to the ICT department.

Approved: ..... **Date:** 27/08/2025

Mrs C. Chigwamba
(COUNCIL CHAIRPERSON)

ACKNOWLEDGEMENT FORM

MARONDERA UNIVERSITY OF AGRICULTURAL SCIENCES AND TECHNOLOGY

I ..... of Department have read the Marondera University of Agricultural Sciences and Technology (MUAST) ICT policy document. I understand the contents and I agree to comply with the said policy.

Location:

.....

Employee/Student Number: .....

Employee/Student Signature..... Date.....

Supervisor Signature..... Date .....