MZUZU UNIVERSITY
ICT POLICY

Table of Contents

POLICY ON THE USE OF MZUZU UNIVERSITY (MZUNI) INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) RESOURCES

1.1 Policy

All Users will be lawful, efficient, economical and ethical in their use of the Mzuzu University's ICT Resources.

1.2 Definitions

a) ICT Resources

All of the University's Information and Communication Technology Resources and facilities including, but not limited to: telephones, mobile phones, email, server space, the Intranet, the Internet, e-Services, computers, printers, scanners, associated peripherals and equipment, any connection to the Mzuni's network, or use of any part of the University's network to access other networks, or other ICT facilities that the University owns.

b) User(s)

All employees, any person enrolled in any course of study at the University and any person registered to attend short courses, seminars or workshops in the University, as well as all other persons including members of the general public, who have been granted access to, and use of, the University's ICT Resources.

NB: A member of the public reading public University web pages from outside the University is not by virtue of that activity alone considered to be a User.

1.3 Principles

a) The University's ICT Resources exist and are maintained to support the university's activities. The University reserves the right to monitor the use of its ICT Resources and to deal appropriately with users who use the same in ways contrary to the conditions of use set out in this policy.

b) The University will exercise its right with regard to web based and other electronic documents in accordance with relevant Laws.

c) While the University strives to protect its ICT resources it for loss or damage, consequential loss or damage, or loss of data arising from the use of its ICT Resources or the maintenance of its ICT Resources.

1.4 Coverage

This policy document applies to all Users of the University's ICT Resources.

1.5 Conditions of Use

Use of the University's ICT Resources is restricted to legitimate University purposes only. For students this generally means academic coursework and research as approved by a supervisor. Staff usage will depend on the nature of their work.
The use of University ICT Resources through non-University (including personally owned) equipment is also subject to this policy.

The examples of prohibited and permitted use are as follows:

a) The University will not tolerate its ICT Resources being used in a manner that is harassing, discriminatory, abusive, rude, insulting, threatening, obscene or otherwise inappropriate.

b) It is illegal to use any ICT Resource to harass, menace, defame, libel, vilify, or discriminate against any other person within or beyond the University.

c) Users may be individually liable if they aid and abet others who discriminate against, harass or vilify colleagues or any member of the public. Users who adversely affect the reputation of another person may be sued for defamation by that aggrieved person.

d) Users must not use the University's ICT Resources to collect, use or disclose personal information in ways that is contrary to the university rules and regulations.

e) Users must respect and protect the privacy of others.

f) Users are forbidden to use ICT Resources to access, store or transmit pornographic material of any sort other than with specific written approval from an authorised University Officer for research related purposes.

g) The University forbids the use of its ICT resources in a manner that constitutes an infringement of copyright.

h) Users must not download and/or store copyright material, post copyright material to University websites, transfer copyright material to others or burn copyright material to CD ROMs or other storage devices using ICT Resources, unless the copyright material is appropriately licensed. Copyright material includes software, files containing picture images, artistic works, live pictures or graphics, computer games, films and music (including MP3s) and video files.

i) ICT Resources must not be used to cause embarrassment or loss of reputation to the University.

j) The University does not permit the use of its ICT Resources for unauthorised profit making or commercial activities and furtherance of personal gain.

k) Users must not use ICT Resources in inappropriate ways, which are likely to corrupt, damage or destroy data, software or hardware, either belonging to the University or to anyone else, whether inside or outside the network. **Note:** This does not apply to specially authorised University computing staff who may be required to secure, remove or delete data and software, and dispose of obsolete or redundant ICT Resources as part of their ICT Resource management duties.

l) Users must not attempt to repair or interfere with, or add any devices (whether hardware or components) to, any ICT Resource, unless they are authorised to do so. All faults or suspected faults must be reported to the ICT Help Desk.

m) ICT Resources must not be used to distribute unsolicited advertising material from organisations having no connection with the University or involvement in its activities.

n) University Email lists generated for formal University communications must not be used for any other business.

o) Files may only be accessed or downloaded if they are work or study related. In any case, files may only be downloaded if it is legal to do so and steps have been taken to ensure that the files are free from viruses and other destructive codes.

p) Files can only be attached to email messages if they are free from viruses malicious or other destructive code.

q) Users must not attempt to gain unauthorised access to any ICT services. The use of another person's login, password credential is not permitted. Users exploit any vulnerabilities in the systems (except authorised staff when checking security of systems as part of their duties) or use any technology designed to locate such vulnerabilities or circumvent security systems.

r) Users must not facilitate or permit the use of the University's ICT Resources by persons not authorised by the University.

1.6 Monitoring

a) Use of ICT Resources is not considered private. Users of ICT Resources should be aware that they do not have the same rights as they would using personally owned equipment through commercial service providers.

b) The University's electronic communication systems generate detailed logs of all transactions and use. All Users should be aware that the University has the ability to access these records and any backups. In addition, System Administrators have the ability to access the content of electronic communications and files sent and stored using the University's equipment.

c) The University reserves the right to audit regularly and monitor the use of its ICT Resources to ensure compliance with this policy.

d) The University also reserves the right to look at and copy any information, data or files (including non-University material) created, sent or received by Users using, or while connected to, the University's ICT Resources in the event of a suspected breach of this or other policies.

e) To include physical security.

1.7 Responses to Breaches

a) The University reserves the right to withdraw, restrict or limit any User's access to its ICT Resources if a breach of these conditions is suspected. Any such suspected breach may also be investigated under other University processes, and may result in disciplinary action being taken

against the offender in accordance with those processes. This may include a request to reimburse costs (e.g. for unreasonable personal use), disciplinary action (including termination of employment/suspension of candidature) and /or criminal prosecution.

b) The University reserves the right to remove or restrict access to any material within the University domain. Such decisions will be communicated to the appropriate supervisor and account holder.

1.8 Security, Confidentiality and Privacy

a) Matters of a confidential nature should only be conveyed or stored in an electronic format when adequate security measures have been taken.

b) While the University communications systems are electronically safeguarded and maintained in accordance with current best practice, no guarantee can be given regarding the protection confidentiality, privacy or security of any information.

c) Email and other records stored in ICT Resources may be the subject of a subpoena, search warrant, discovery order or application.

d) Communications on University business in any format or media are official records. This includes email sent and received by staff members on any University related matter. Staff needs to be conscious of the need to preserve official communications. Care should be taken before deleting any electronic communication that it is not required to be kept as evidence of a decision, authorisation or action.

e) Sending an email on an official University matter is similar to sending a letter on University letterhead. Such email transactions should be handled with the normal courtesy, discretion and formality of all other University communications. Users should not write anything in an email that they would not sign off in a memorandum.

1.9 Approval

By

_____ _____

Council **Date**

Date of Effect _____

1.10. Amendment and Review

Proposed Date of Review 12 months from date of approval

2.0 SOCIAL MEDIA POLICY

2.1 Introduction

The term “social media” refers to a set of online tools that supports social interaction among users. These include but not restricted to Facebook, Twitter, Flicker, YouTube, Instagram etc.

Social media has radically changed the way we communicate and interact. It offers opportunities to connect and engage with a range of key stakeholder groups including prospective and current students, staff, alumni, donors, research collaborators and friends of the University.

Mzuni currently maintains social media presence on Facebook, and Twitter. However the University is in the process of broadening presence through other social media networks.

Mzuni welcomes the use of social media to facilitate knowledge and information sharing, among users and the general public. The University recognises that inappropriate use of social media has the potential to damage its image, reputation since the lines between personal voice and institutional voice can be blurred on social media platforms.

This Policy is intended to assist the University to achieve maximum benefits while minimising risks of social media networking. This Policy aims to exert positive influence on and help shape the online social behavior of the University community in physical and virtual spaces or while using facilities that are owned and/or controlled by the University.

2.2 Purpose

This Policy outlines the Mzuni's position on the appropriate use of social media by members of its community. It seeks to clarify how best to enhance and protect personal and professional reputations when participating in social media. It serves to facilitate and encourage the proper use of social media while sensitizing users about the risks of antisocial activity with a view to protecting Mzuni from liability that may be vicariously incurred when members of the community misuse Mzuni's Information and Communications Technology (ICT) systems.

2.3 Scope

This is a University-wide policy and shall apply to all Mzuni Departments/Sections, Centre, and bodies such as Staff and Students Associations and all users of the University ICT systems.

This Policy applies to all Mzuni Social Media Sites and to the activities permitted by these sites. It applies to sites and any activity that falls within the genus of social media, whether they are current or come into existence on or after the date of the approval of this Policy. Examples include weblog posts (blogging), event updates, news updates, chats, discussion boards/posts, photo/video sharing, music and radio broadcasts and gaming.

2.4 Statement of Liability

Mzuzu University shall not be liable for any errors, omissions, loss or damage, including indirect and/or consequential loss and/or damage claimed or incurred due to any use of any social media site that does not comply with this Policy or the policies cited herein.

2.5 Policy Statements

This section explains the Mzuni's position on social media and its response to various issues which may arise in the event of inappropriate use of social media by users

2.5.1 Use of the Mzuni Marks

(i) Mzuni Marks include; The Mzuni name, and all other words, logos, signs or any other marks whether registered or not, that belong to or are associated with Mzuzu University.

(ii) Use of Mzuni Marks without permission is illegal. ICT Directorate is the authorized agency (acting on behalf of the University Registrar) from which persons or entities wishing to use Mzuni Marks should seek permission.

(iii) Mzuni Marks shall only be used on social media sites designated as "Mzuni Social Media Sites".

2.5.2 Applicable Laws

Persons making postings shall respect the laws relating to copyright and other intellectual property rights, defamation, privacy, and other applicable laws.

2.6 Content

2.6.1 Compliance with other Mzuni policies

(i) Information published on social media sites should conform to all applicable Mzuni policies, including but not limited to:

a. Acceptable Use Policy, Information and Communication Technology

b. Electronic Mail and Messaging Services Policy

c. Policy on Intellectual Property

d. Policy on Gender Issues

e. Web Policy

(ii) Content posted by users shall conform to The University's principles of confidentiality and information disclosure which are included in the relevant rules and regulations for both staff and students.

2.6.2 Considerations when discussing work-related activities on social media

(i) As a general principle, content posted on any social media site should conform to the tenets of good taste.

a There shall be no posting of biased statements on matters such as politics, religion, race, gender, sexual orientation, nationality or disability.

b There shall be no posting of statements that contain obscenities or vulgarities or that can cause anxiety and panic.

c Statements posted should follow Mzuni's non-biased position and be respectful at all times.

(ii) User should noted that all Mzuni Social Media Sites represent Mzuni. Therefore, content providers must ensure that information placed on any Mzuni Social Media Site is accurate and represents the values of Mzuni.

(iii) Users are reminded of their duties and obligations to maintain staff, student and third party confidentiality and shall not use social media sites to transmit or discuss confidential information, such that users shall conform to the Mzuni's principles on confidentiality and information disclosure.

2.6.3 Compliance Requirements

(i) This policy does not include matters related to the use of social media to support teaching and learning at Mzuni.

(ii) Mzuni entities, lecturers or other personnel interested in supporting their taught courses with social media should not initially seek to establish separate social media accounts, but should first determine whether existing facilities may be utilized and should contact the ICT Directorate at Mzuni for guidance.

(iii) Mzuni entities, lecturers or other personnel already using social media for teaching and learning should have their sites reviewed/assessed by the ICT Directorate to ensure compliance with Mzuni's policies.

(iv) Mzuni entities, lecturers or other personnel already using social media for purposes other than teaching and learning should have their sites reviewed/assessed by The Director of ICT.

(v) Any user desirous of using social media should consult the Director of ICT for appropriate guidance prior to use.

2.7 Penalties for Misuse

Where there is evidence of misuse of social media, Mzuni may restrict or prohibit the use of its ICT resources and/or, where appropriate, request external entities to take action against offenders.

Users who breach this Policy may face disciplinary action (as outlined in the code of conduct on the use of Mzuni ICT Resources) up to and including

termination of employment in the case of staff members; and suspension or expulsion in the case of students.

2.8 User Acceptance

All users of Mzuni's ICT resources are required to signify acceptance of Mzuni's ICT Policies. Mzuni's Social Media Policy & Guidelines are included in the list of Mzuni's ICT Policies governed by the following User Acceptance Clause:

2.9 User Acceptance Clause

I _____ accept the conditions of use as outlined in this Mzuni ICT policies.

Signature: _____

Date: _____

3.0 ICT SECURITY POLICY

3.1 Introduction

In accordance with its broader strategic objectives, Mzuzu University, [hereinafter "Mzuni"] has procured and implemented various, Information and Communication Technologies (ICTs) that are used to create, process, store, share and disseminate data and information. These assets represent a significant economic investment by Mzuni. The data and information resources they create, store and disseminate could well be priceless and irreplaceable. Their continued availability in furtherance of the Mzuni's business is of paramount importance, hence, there is a compelling need to secure and control access to them.

Users of Mzuni ICT Resources and other stakeholders have an expectation of privacy for their personal data gathered by the Mzuni in the normal course of its business. Therefore, there is a reasonable expectation from users that the Mzuni would institute controls to conserve the privacy of personal information. Confidentiality of information is demanded by the common law, national statute as well as university ordinances, regulations and convention. Since the Mzuni operates on an international stage offering higher education services in a global marketplace, misuse of the Mzuni's ICT assets could degrade its goodwill and reputation.

Mzuni acknowledges that there is a well-founded requirement to maintain the integrity and confidentiality of its electronic data and information. Such assets must be protected from unauthorized access and intrusions, malicious misuse, inadvertent compromise and intentional damage or destruction. Accordingly, Mzuni is obliged to ensure that appropriate security measures are enacted for all electronic data and information, as well as ICT equipment and processes in its domain of ownership and control.

3.2 Purpose

This policy is prepared for the direction and use of personnel engaged in the implementation and support of Mzuni's ICT systems and the services delivered thereon. It is intended to inform:

- the development and implementation of rules, guidelines and a code of practice to secure the Mzuni's ICT resources and services;
- the development of mechanisms that will help the University to reduce its legal risk brought about by an increasingly interconnected world;
- users about the rules and practices pertaining to confidentiality and security of the University's ICT resources;
- custodians of University ICT resources and services about their responsibilities with respect to the preservation of these systems and the sanctions for non-compliance.

3.3 Scope

This policy outlines the requirements for securing Mzuni's data and information assets and provides the groundwork for the development of local policies, guidelines and best practices insofar as it is practical. This policy applies to the mitigation of the following categories of risk:

- Computer system availability
- Conservation of Mzuni ICT resources
- Integrity and confidentiality of University data and information
- Efficient use of Mzuni ICT resources

It covers the following security domains:

- The physical security of all computing and communication premises, computers, communication equipment and appliances, transmission paths and computer peripherals.

- The physical security of all storage media for data, system software, application software and documentation.
- The physical security of power systems supplying electrical power to network communication and computer systems.
- The logical security of data, information and information processing resources such as databases, computer programs, email records, servers, routers, switches and other network appliances.

3.4 Roles and Responsibilities

ICTs are provided and deployed by Mzuni to support its operational and administrative functions of Teaching, Learning, Research, as well the management of its business. They are intended to be used primarily as business tools and to provide other support services.

3.5 General

The ICT resources deployed are University facilities. All such technologies are and remain the property of the Mzuni, hence certain assigned Intellectual Property rights are excepted.

3.6 Roles

The ICT Directorate shall:

- Account for all ICTs and information resources in their area of jurisdiction that is connected to campus networks by one or other means.
- Provide and maintain a database of unique identifiers for all network-connected ICT assets.
- Assess the security risk of all ICT systems and apply such security systems and processes as are consistent with the mitigation of this risk.

- Provide and/or commission the physical security of all enterprise servers, databases, backbone network switches and ICT management, teaching and learning platforms.
- Procure, implement and maintain the logical security systems as are necessary to protect University electronic data and information assets from misuse, damage, loss or unauthorized access.
- Develop, document and publish the ICT security guidelines in accordance with and
  informed by best practice.
- Promote a security awareness campaign for users of University ICT systems and collaborate with functional departments to design and deliver end user ICT security awareness training.

Heads of Departments with functional ownership of data and information resources shall:

- Assess the security risk to data and information resources developed, generated and produced in their operations
- Determine the confidentiality requirements for data and information resources developed, generated and produced by their departments
- Collaborate with University and ICT Directorate to develop and implement procedures that establish and manage privilege to access confidential data and information resources
- Ensure every user in their jurisdiction and span of control is informed of the security requirements

3.7 Responsibilities

a) The ICT Directorate is responsible and accountable for all aspects of the design, implementation, administration and maintenance of all ICT security systems and the processes and procedures by which these operate. It has the duty to immediately suspend privilege, access and service to any user in breach of this policy pending further enquiry. Such restrictions as applied are subject to review by the appropriate superior university authority

b) Users of the services are responsible for maintaining the security of their interfaces to University-owned ICTs, data and information resources by complying with University policies and regulations, and related national and international laws. Persons found to be in violation of this policy may be liable to disciplinary action under University regulations and ordinances. Violation may also constitute a breach of national law.

c) Functional Managers and Heads of Departments are responsible for enforcing the application of the security policies covering ICT resources, data and information resources as set out in local guidelines and practice documents

3.8 Physical Security & Integrity of Systems

- Appropriate barriers and controls governing the physical access to, and the maintenance of, the integrity of critical University ICT assets must be deployed commensurate with the risk identified. These risks include identified natural and environmental hazards.

- Barriers and controls include, but are not limited to, electronic access control to servers and critical network infrastructure, installations of grillwork surrounding and enclosing video systems, fire suppression, and power management systems.

- Physical ICT assets include but are not limited to multifunction devices, servers, communication switches, personal computers, cameras, printers, plotters, multimedia projectors, media management platforms, scanners, media containing software, books and manuals.

3.9 Logical Security & Integrity of Systems

- Authentication and authorization functions must be employed for all users of University electronic data and information resources.

- A central authentication database shall be established for all users.

- Procedures to manage access, authentication and authorization shall be developed to support and manage these activities. Such processes and procedures include but shall not be limited to MAC authentication of devices on the network, user passwords for network and application access, biometric access mechanism, tokens and electronic key devices. For the purposes of this paragraph, computer and other electronic processes are deemed to be users.

3.10 Software and Firmware upgrades

All computers, switches, routers and other network-attached devices shall have the most recent approved and released software and firmware security patches installed as soon as they are generally available.

3.11 Malware control

Malware is a common feature of globally connected networks. Personnel engaged in the implementation and support of the Mzuni's ICT systems shall take all appropriate steps to protect its ICT assets from damage, compromise or loss of confidentiality. For the purposes of this policy, malware is defined as software agents that by their action deny users the maximum capabilities of the ICT systems, compromise the security and confidentiality of university data and information or destroy or damage university ICT assets. Malware may be represented by but is not limited to spyware, viruses, worms and spam.

3.12 Network Interconnections

Interconnections among networks are unavoidable in the ordinary course of business. These interconnections are portals for unauthorized access and entry to University networks and pose significant risk to the security of University data and information resources. Therefore all network interconnections shall be guarded, and audited by processes and such perimeter defence and intrusion detection systems, as are appropriate to manage and mitigate these risks.

3.13 Access to Business Critical systems

The University is dependent on several of its major systems for its daily operations. Breaches to their integrity, or their unavailability for any significant period of time, could reduce the service delivery capability or place the institution in disrepute. Such systems may include the Student Administration System, online teaching and learning platforms, the financial management system, the Library Management system. Notwithstanding the general security safeguards enunciated before, these business-critical systems shall be provided with an elevated level of security. These additional measures shall include, but are not limited to, internal firewalls. When the security requirements are stringent enough, internal isolation of the network segment to which such systems are attached is the final consideration.

3.14 Privacy and Confidentiality

Mzuni requires that the architecture, processes and procedures surrounding applications must be such that privacy of University data and information is protected. Users of University applications must be advised of the procedures required to maintain privacy of University data and information.

3.15 Right to monitor ICT systems

Notwithstanding Mzuni's acknowledgement of an inherent right to privacy by users of the University ICT systems, the University reserves the right to monitor, audit and interdict all electronic payloads traversing its networks or stored on its systems in furtherance of its duty to secure and retain the confidentiality of its data and information resources.

3.16 Localised Policies

Notwithstanding the broad elements of this policy, Departments/Sections may establish or seek to establish complementary policies, standards, guidelines or procedures that refine or extend the provisions of this policy and to meet specific local needs. In any event, such extensions shall comply with university regulations, ordinances and national laws.

4.0 MZUZU UNIVERSITY ICT USER AGREEMENT

4.1 Network user agreement

When a 'User' logs on to the network at the Mzuzu University they agree to adhere to the following guidelines.

4.2 General

You will:

i. be the sole person authorised to use this User ID;

ii. be solely responsible for all actions taken under your User ID while it is valid;

iii. not let others use your User ID and your Password nor inform others of your User ID or Password;

iv. not delete, examine, copy or modify files and/or data belonging to other users without their prior consent;

v. not deliberately impede other users through mass consumption of system resources;

vi. not take any unauthorised, deliberate action which damages or disrupts an ICT system, alters its normal performance, or causes it to malfunction, regardless of system location or time duration;

vii. Accept that, data stored on the Network can be moved internally by qualified staff in ICT Services.

4.2 Electronic Mail

You will :

i. be responsible for all electronic mail originating from your User ID;

ii. not forge, or attempt to forge, electronic mail messages;
iii. not attempt to read, delete, copy or modify the electronic mail
iv. directed to other users without prior consent;
v. not send, or attempt to send, harassing, obscene and/or other threatening e-mail to another user of any e-mail service. Further information can be found in the University's E-Mail and Internet Policy;
vi. not send 'for-profit' messages or chain letters.

Further information regarding the University Electronic Mail and Messaging Services Policy which is detailed later in this document.

Network Security

You will not :

i. Use University Systems in an attempt to gain unauthorised access to remote systems;

ii. attempt to gain unauthorised access to University Systems from remote systems;

iii. attempt to decrypt the system or user passwords;

iv. copy University System Files;

v. attempt to 'crash' University Systems or programs;

vi. attempt to secure a level or privilege on University Systems higher than authorised;

vii. load programs or computer software applications onto the University Systems or computer hard disk without the written authorisation of the ICT Director;

viii. Wilfully introduce computer 'viruses' or other disruptive/destructive programs into the University Systems or into external networks.

ix. Use non-University ICT equipment on the Network.

4.3 ICT Policy Framework

The Framework requires that you:

i. are aware of the University Information and Communications Technology Policy Framework including all its constituent parts and accept its terms and conditions;

ii. accept that violation, or attempted violation, of your responsibilities as a user may lead to your exclusion from the System;

iii. have read and understood this User Agreement and accept full legal responsibility for all of the actions that you commit using the University's Systems according to any and all applicable laws;

iv. understand that from time to time the University Systems and attached equipment may fail unexpectedly while you are using them and you will not hold the University responsible for lost time or data.

5.0 ICT BREACH POLICY

5.1 Introduction

All users granted access to or use University Information and Communication Technology (ICT) resources shall use these facilities and services in an appropriate and responsible manner. The University reserves the right to record and monitor activity, limit, restrict, cease, or extend access of ICT facilities and services.

Disciplinary actions apply, for violation of the Mzuzu University ICT Acceptable Use Policy and/or procedures. Any alleged breach of the Acceptable Use Policy, at any of MZUNI's entities, shall be reported to ICT Directorate who will record, investigate and act in accordance with this (ICT Breach) policy.

5.2 Objectives

a) To ensure consistent and expedient investigation and management of alleged breaches.
b) To ensure that ICT resources are used in an appropriate and responsible manner.
c) To safeguard the integrity and security of the ICT resources.

5.3 Management of breaches

5.3.1 Breach Reporting

Any reported information security incident that is considered to be an alleged breach of ICT policy or procedures will be classified as (i) minor breach or (ii) major breach (see Schedules A and B).

All breaches shall be investigated to determine whether a breach was of an accidental or deliberate nature.

Consistent classification of breaches and recommended disciplinary actions across the University shall apply. Guides to the applicable response are described in the following Schedules:

- Breaches by Staff: Schedule A.
- Breaches by Students: Schedule B.
- Example categorisation of breaches: Schedule C.

5.3.2 Breach Management Reporting

a) Periodic management summary reports of breaches shall be published.
b) Priorities shall be assigned to breaches based on the severity of the impact on the University.
c) Confidentiality of information related to individual users shall be maintained at all times.

5.3.3 Breach penalties

5.3.3.1 Internet breach

Depending on the type and circumstances of an Internet use breach the following external access restriction penalties will apply:

- Password/Account - 20 days,
- Pornography - 14 days,
- Copyrighted Content - 14 days,
- All other - 7 days (after first warning)

Pornography and Copyrighted Content repeat breaches will incur a 20 day external Internet limited access restriction and will be subject to ICT Breach Policy action. As necessary, University network or external Internet access may be completely suspended.

Depending on the breach history, subsequent breaches may result in external Internet access being fully restricted and escalation to the appropriate authority for disciplinary action.

Recovery of internet traffic costs as a result of a breach shall be considered and auctioned where appropriate.

5.4 Schedule A – categories of breach for staff

5.4.1 Minor Breach

Example of Policy Breach	First Breach	Subsequent Breach
Any activity considered by the staff member's Department/Section or nominee and the ICT directorate representative as inconsistent with the staff member's responsibilities	• Email warning and recipient acknowledgement • Interview optional	• Optional notification to relevant officer or Head of Department • Staff disciplinary procedure

5.4.2 Major Breach

Example of Policy Breach	Action
Any audio-visual copyright breach e.g. music, films, videos	Staff disciplinary procedure
Use of copyright software outside the University's License provisions	Staff disciplinary procedure
Giving access to restricted material to a minor/s	• Staff disciplinary procedure • Anti Corruption Bureau or Police to be advised
Viewing, downloading, storing, distributing and/or giving access to objectionable material	• Staff disciplinary procedure • Anti Corruption Bureau or Police to be advised

5.5 Schedule B – Categories of breach for students

5.5.1 Minor Breach

Example of Policy Breach	First Breach	Subsequent Breach
Any activity considered by the student's Department/Section Head or nominee and the ICT directorate representative as inappropriate and irrelevant to the student's academic progress	• Email warning and recipient acknowledgement • Interview optional	• Optional notification to relevant officer or Head of Department • Student disciplinary procedure

5.5.2 Major Breach

Example of Policy Breach	Action
Any audio-visual copyright breach e.g. music, films, videos	Staff disciplinary procedure
Use of copyright software outside the University's License provisions	Staff disciplinary procedure
Giving access to restricted material to a minor/s	• Staff disciplinary procedure • Police to be advised
Viewing, downloading, storing, distributing and/or giving access to objectionable material	• Staff disciplinary procedure • Police to be advised

NOTE: Any information security incident where a legal infringement is suspected MUST be dealt with as a Major Breach.

5.6 Schedule C - Example categorisation of breaches

This schedule provides a guideline on breach types and breach categories.

Breach type	Category
Doing anything dishonest or illegal. E.g. plagiarising an assignment (i.e. presenting someone else's work as your own).	Major
Copying or sharing with others software, music or movies without the written permission of the copyright owner. Some examples include, but not restricted to: • Copying or sharing sound recordings, films, videos, radio and television broadcasts via email, CD or other electronic means. • Making a CD track or movie available via a file-sharing service (e.g. peer-to-peers), an FTP service, or a web-site. • Copying a videotape, CD, or DVD onto another videotape, CD, DVD, computer hard disk, or any other storage device. • "Ripping" a music track to a Mzuzu University disk or duplicating a music CD. • Copying a computer file containing music or video onto a videotape, CD, DVD, computer hard disk, or any other storage device. • Downloading a CD track or movie from a file-sharing service (e.g. a peer-to-peer service), an FTP service, or a web-site. • Storing a file on University equipment that contains illegally copied software, music or video storing of files on a personal piece of equipment, copyrighted software or audio visual material accessed using the Universities Internet service.	Major
Hacking into, meddling with, or damaging any other computer or service. e.g. trying to "break into" or "crash" another computer on the Internet.	Major
Using another person's identity or authorisation codes. e.g., using someone else's username or password.	Major
Possessing, accessing or using any unauthorised hacker tools, whether hardware or software based. e.g. "packet sniffers" and "password crackers".	Major
Viewing, downloading, storing, sending, or giving access to material deemed as objectionable by the Malawi Censorship and Control of Entertainment Act. e.g. materials such as child pornography, incitement to violence, torture, and bestiality.	Major

Giving an underage person under the age of eighteen years access to material regarded as restricted by the Malawi Censorship and Control of Entertainment Act. e.g. materials involving sex, drug misuse or addiction, crime, cruelty, and violence.	Major
Harassing any person. E.g. sending obscene messages, language, pictures or other materials; issuing threats of bodily harm; contacting a person repeatedly without legitimate reason; disrupting another person's lawful pursuits; and invading another person's privacy.	Major
Unauthorised use of access accounts and/or passwords	Major
Theft of any Mzuzu University ICT hardware and software	Major
Unauthorised viewing, downloading, storing, sending, distributing or giving access to Restricted material using Mzuzu University ICT resources e.g. CDROM, USB etc	Minor
Unauthorised use of peer-to-peer software	Minor
Obstruct other students from using computers in a Mzuzu University student computer laboratory. E.g. by using it for anything other than academic and research activities	Minor
The use of Mzuzu University ICT resources for the playing of games or chat sessions not associated with the teaching, learning, research or administrative functions of the University.	Minor

ICT Breaches are not necessarily limited to those outlined above.

6.0 ELECTRONIC MAIL & MESSAGING SERVICES POLICY

6.1 Introduction

In accordance with its broader strategic objectives, The University of the West Indies (the MZUNI) promotes the use of electronic mail services to share information, improve communication, and to exchange ideas.

6.2 Purpose

This policy is prepared for the direction and use of all users of the MZUNI's electronic messaging services. It is intended to ensure that:

- Rules and guidelines are established for the MZUNI's electronic messaging services;
- The MZUNI community is informed about the rules governing e-mail derived from or entering the MZUNI's electronic messaging system.

Users of electronic messaging services are informed of their responsibility for compliance with these rules and regulations.

6.3 Scope

This policy outlines the requirements for the use of electronic messages and adheres to best practices as far as is practical. It applies to:

- All electronic mail systems and services provisioned or owned by MZUNI;
- All users, holders, and uses of the MZUNI electronic messaging services; and
- All MZUNI e-mail/electronic messaging records in the possession of MZUNI employees or other authorized users of electronic messaging services provided by the MZUNI.

6.4 Ownership and Responsibilities

Electronic messaging services are provided by MZUNI to support its functions i.e. teaching, learning, research, and the management of the MZUNI's business.

6.5 General

MZUNI electronic mail systems and services are university facilities. All e-mail addresses and messaging IDs maintained by the system are the property of Mzuzu University.

6.6 Copyright Laws and License Agreements

Notwithstanding the foregoing, MZUNI shall respect the provisions of its Intellectual Property and Ethics Policies and the users of the system shall observe these Policies and all applicable copyright laws and license agreements.

In addition users should not:

i Reproduce an email message in full when responding to it, especially if they are posting to a bulletin board.

ii Extract and use text from someone else's message without acknowledgment

iii Make changes to someone else's message and pass it on without making it clear where they have made changes

6.7 Responsibilities

a) The ICT Directorate is responsible for all aspects of the design, implementation and maintenance of the electronic messaging system and its operation.

b) ICT Directorate in collaboration with Heads of Departments/sections are responsible for enforcing the application of the electronic messaging policies throughout the university.

c) Users of the services are responsible for managing their messages and complying with University policies as well as related national and

international laws. Persons found to be in violation of this policy will be subject to disciplinary action.

6.8 Authorized Users

Users of Electronic Messaging Services are to be limited to MZUNI students, faculty, staff and other approved persons, for purposes that advance the objectives of teaching, learning, research, outreach and administration.

6.9 Use of Email/Messaging Accounts

All email/messaging accounts shall conform to the information security procedures defined and implemented from time to time and managed by the ICT Directorate.

6.10 Login Credentials

Passwords should not be given to other persons.

6.11 Access to Mzuni E-Mail/Messaging Services

Access to university electronic mail services, when provided, is a privilege that may be wholly or partially restricted by order of the Competent University Authority without prior notice and without the consent of the e-mail/messaging user when there is substantiated reason to believe that violations of policy or law have taken place. Such restriction as applied is subject to review from time to time.

6.12 Email Messaging Content

The content of electronic messages qualifies as recorded material and is subject to the same rules and regulations as any other type of record created, used, or received and retained by the University.

6.13 Creation of Messages

a) The same rules governing good sociable behaviour applying to face-to-face communication or to traditional written communication, apply also to electronic communication.

b) Messages should reflect careful, professional and courteous drafting, particularly since they are easily forwarded to others.

c) It is advised that every user of university email/messaging systems assume that others than the addressee[s] may read a message.

6.14 University Records

a) Messages sent or received on behalf of the University and which provide evidence of an activity, transaction or event must be regarded as official University records.

b) Messages sent or received shall be retained in the official repository. Their disposal must be in accordance with approved retention and disposition schedules.

c) Records relative to matters subject to on-going or threatened legal action or any investigation must be retained and should not be disposed of, even if the retention period has been met on the records retention schedule, except as advised by the University Legal Counsel.

6.15 Offensive Electronic Content

It is strictly prohibited to send harassing, abusive, intimidating, discriminatory or other offensive electronic messages. It is a misuse of the facilities, and may in certain cases, be illegal for a user to receive, transmit, display or store such offensive material using ICT Resources.

Such misuse may result in disciplinary or legal action being taken against those responsible.

6.16 Responsible Use

a) Users of university electronic messaging systems are expected to exercise sound judgment and caution when distributing electronic messages.

b) Users should immediately report misuse or security breaches detected to their department/section heads and/or to ICT Directorate.

c) Heads of Departments/sections shall address reported breaches or refer these to the Director of ICT.

6.17 Restrictions

The Electronic messaging services may not be used for:

- Unlawful activities or those that cause interference with other users;
- Commercial purposes not under the auspices of the University;
- Personal financial gain, except as permitted by the University;
- Personal use inconsistent with Mzuzu University policies;
- Uses that violate other University's policies or guidelines. This includes, but is not limited to, policies and guidelines regarding intellectual property, or policies regarding harassment in any form.

6.18 Misrepresentation

a) E-mail users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the University or any unit of the University unless appropriately authorized (explicitly or implicitly) to do so.

b) Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing the University.

6.19 Personal Use

Although the University's electronic messaging system is meant for university business use, the University shall allow the reasonable use of its electronic messaging systems for personal use if certain guidelines are adhered to:

- Personal use of the electronic messaging system should not interfere with work.
- Personal electronic messages must conform to these policies and accompanying guidelines.
- Personal electronic messages are advisedly kept in a separate folder and deleted regularly.
- Users should restrict the number of personal emails sent within working hours.
- Mass mailing is not allowed.

6.20 Electronic Messaging Etiquette

The following is a summarised list of *Do's* and *Don'ts* to help promote a code of good electronic messaging practice in the University.

Do's

i Check your mail regularly

ii Always reply, even if the reply is brief

iii Try to reply promptly to avoid any confusion about whether an e-mail has been received

iv Develop an orderly filing system for email messages you wish to keep, and delete unwanted ones to conserve the allocated 100Mb/20Mb of server disk space

v Try to keep email messages fairly brief, *(max. 2 screen fulls)*

vi Try and make sure that the *"Subject"* field in email messages is meaningful, to help put the e-mail into context. Also, when the reply option is used, ensure that the subject field still accurately reflects the content of your message

vii Try to restrict yourself to one subject per message, this helps recipients to use the "subject" field to manage their messages

6.21 Security and Confidentiality

The ICT Directorate shall follow sound professional practices in providing for the security of the electronic messaging system under their jurisdiction. Since such professional practices and protections are not fool proof however, the security and confidentiality of electronic mail cannot be guaranteed.

Users should therefore be aware that confidentiality may be compromised, by application of law or policy, including this Policy, by unintended redistribution, or because of inadequacy of current technologies to protect against unauthorized access. ***Consequently, extreme caution should be exercised in using electronic messages to communicate confidential or sensitive matters.***

6.22 Privacy

a) The university reserves the right to monitor ALL electronic messages and to protect itself from any liability due to the unlawful use of the services provided.

b) Users should be aware that during the performance of their duties, network and computer operations personnel and system administrators, may need to, periodically, observe certain transactional addressing

information to ensure proper functioning of the university e-mail/messaging services, and on these and other occasions may inadvertently see the contents of email messages.

6.23 Security Protection

a) The University attempts to provide e-mail/messaging services which are as secure and reliable as practical and as the technology allows. Users are required to assist in the security of their files by employing good password management and usage practices as described in the guidelines accompanying this document.

b) Users should report any strange or suspicious e-mails/messages using proper channels to the ICT Directorate.

c) Any suspicious URL links and attachments are not encouraged to be opened by the user of email/messaging systems and this must be reported accordingly.

DECLARATION

I have read, understood and now acknowledge receipt of the E-mail policy. I will comply with the provisions of, and accompanying guidelines to, this policy; and understand that failure to do so might result in disciplinary or legal action being taken against me by the University of the West Indies.

Signature: _____ Date: _____

Printed Name: Campus/Department/Faculty/Unit: