WOMEN'S UNIVERSITY IN AFRICA

Addressing gender disparity and fostering equity in University Education

ICT POLICY MANUAL

Version 2.0

TABLE OF CONTENTS

REVISION HISTORY

Revision	Date	Description of changes
2.0	23/07/2025	Review of the entire ICT Department policy framework

1 INTRODUCTION

In pursuing its mission of reducing gender disparity, the Women's University in Africa (WUA) makes use of information and communication technologies to manage its knowledge resources. To ensure efficient and effective utilisation of information and communication technologies, WUA provides policies, regulations and guidelines that facilitate and regulate the way the stakeholders use the ICT resources. This policy manual details the following policies:

a. Acceptable use of ICT resources policy
b. Bring your own device policy (BYOD)
c. Electronic communications policy
d. Security management policy
e. ICT asset management and disposal policy
f. Software policy
g. Artificial Intelligence (AI) policy
h. Electronic learning policy
i. Electronic recording of meetings policy
j. Change management policy

This ICT Policy Manual has been developed in full alignment with the provisions of the Zimbabwe Cyber Security and Data Protection Act [Chapter 12:07], ensuring that the University's ICT operations uphold national legal standards for cyber governance, data protection, and responsible digital conduct. In particular, the manual reflects compliance with Section 4, which mandates the lawful and fair processing of personal data—this is directly embedded in university practices concerning the collection, storage, and use of student, staff, and stakeholder information. Section 18 on Data Security is operationalised through institutional safeguards against data breaches, including strict access controls and incident response protocols within the ICT infrastructure. The policy also incorporates Part IV, which relates to the obligations of data controllers, by clearly assigning responsibility to ICT personnel for ensuring that data processing adheres to the principles of integrity and confidentiality. Furthermore, the acceptable use provisions are guided by Section 164 of the Criminal Law (Codification and Reform) Act as referenced in the Cyber Security Act, discouraging unauthorised access, system interference, and misuse of ICT resources. Through this policy manual, the University affirms its commitment to fostering a secure, ethical, and legally compliant digital environment in line with national cyber legislation.

1.1. POLICY STATEMENTS

1.1.1. ACCEPTABLE USE OF ICT RESOURCES POLICY

It is University policy to:

1.1.1.1. Leverage on technology in all business activities.

1.1.1.2. Provide affordable and appropriate ICT resources to support business activities.

1.1.1.3. Protect information privacy and confidentiality.

1.1.1.4. Establish access levels, rights, privileges, obligations, prohibitions and sanctions consistent with the University Information and Communication Policy, aimed at enabling easy access to corporate data and information needed for the different roles of the University community, while assuring the integrity of such data and information and respecting the privacy of individuals.

1.1.1.5. Require all Clients and ICT personnel to always conduct themselves in an ethical, professional and responsible manner.

1.1.1.6. Monitor and enforce acceptable use of ICT resources.

1.1.2. BRING YOUR OWN DEVICE POLICY

1.1.2.1. It is University policy to encourage all University Clients, especially students, to use their own devices to access selected ICT services availed by the University to enable timely access to information.

1.1.2.2. This policy does not replace the obligations of the University to provide computing services and devices for use by students and staff.

1.1.3. ELECTRONIC COMMUNICATIONS POLICY

1.1.3.1. It is University policy to facilitate clear, efficient, and effective communication within the University community, including staff, students, and external stakeholders. Using electronic communication platforms

1.1.4. SECURITY MANAGEMENT POLICY

It is the University policy to

1.1.4.1. Protect facilities and assets from unauthorized access, theft, and vandalism.

1.1.4.2. Protect data integrity, confidentiality, and availability

1.1.4.3. Ensure security measures comply with relevant local regulations and statutory instruments.

1.1.4.4. It is University policy to protect the privacy and ensure security of personal data of its students, staff, and other stakeholders.

1.1.5. ICT ASSET MANAGEMENT AND DISPOSAL POLICY

1.1.5.1. It is the University policy to ensure the effective stewardship of its ICT resources, supporting its mission and safeguarding its technological investments.

1.1.6. SOFTWARE POLICY

It is University policy to

1.1.6.1. Ensure that all software used in the institution is appropriately licenced.

1.1.6.2. Prohibit any unauthorised use or copying of software.

1.1.6.3. Conform to software usage according to licencing agreements and general University guidelines.

1.1.6.4. Ensure security and continued functionality of software through regular updates and upgrades.

1.1.6.5. Guarantee that all software purchases are approved by the ICT department for compatibility, security and compliance with University standards.

1.1.6.6. Vet all software and platforms for vulnerabilities before installation.

1.1.7. ARTIFICIAL INTELLIGENCE (AI) POLICY

1.1.7.1. It is University policy to promote the responsible development, deployment, use and governance of AI technologies in accordance with ethical principles and best practices.

1.1.8. ELECTRONIC LEARNING POLICY

1.1.8.1. It is University policy to improve the quality and availability of teaching and learning by leveraging appropriate technologies.

1.1.9. ELECTRONIC RECORDING OF MEETINGS POLICY

1.1.9.1. It is University policy to promote and/or cause the recording of approved teaching and learning activities, the administration, processing and storage of the content thereof.

1.1.10. CHANGE MANAGEMENT POLICY

1.1.10.1. It is University policy that ALL changes, new services, enhancements or amendments to any platform or service including cloud services go through a change management process.

2 ACCEPTABLE USE OF ICT RESOURCES POLICY

2.1. INTRODUCTION

The University makes use of electronic information and communications technologies (ICTs) and makes them widely available to the University community. Nonetheless, the use of electronic communications resources requires clear definition and enforcement of policies and guidelines which outline acceptable and unacceptable uses of ICTs at WUA.

2.2. INTERPRETATION (DEFINITION OF TERMS)

The terms and definitions below are specific to this policy and are critical to its effectiveness:

2.2.1. **Acceptable use:** The responsible, ethical, and authorized use of institutional ICT resources—such as computers, networks, internet access, software, and digital content—in a manner that supports the mission of the Women's University in Africa in teaching, learning, research, innovation, industrialisation, community outreach and administration, while complying with applicable laws, University policies, and professional standards.

2.2.2. **Clients:** includes Staff, Student, Alumni or Affiliates who, based on their relationship with the University, need to be granted access to University ICT resources.

2.2.3. **Staff:** are defined as individuals who hold an active employment contract with the University and are present in the University's Human Resources and Payroll System.

2.2.4. **Student:** defined as an individual who is currently enrolled in a program at the University and exists in the University's Academic Registry Information System. However, where explicitly stated, student may include an applicant to the University, a student on study deferment or those individuals undertaking short term study programs

2.2.5. **Alumni:** a former student who has completed their program and are present in the University's Academic Registry Information System with status of Graduate

2.2.6. **Affiliate:** defined as an individual who has a bona fide relationship with the University for which approval has been gained to offer access to various ICT resources. This may include adjunct or visiting appointees, volunteers, contractors and consultants.

2.2.7. **ICT Resources:** includes a range of information and communication technology hardware, software and services that may be owned, contracted, licenced, managed or otherwise facilitated by the University to be used by the University community and its authorised clients.

2.2.8. Undesirable Content: Any digital material or online resource that is inappropriate, offensive, illegal, or otherwise inconsistent with the values, goals, and operational integrity of the Women's University in Africa. This includes, but is not limited to, content that is pornographic, violent, discriminatory, defamatory, harassing, promoting hate speech, enabling cybercrime, compromise security, disrupt productivity, infringing on intellectual property rights, violate national laws, University regulations or professional ethics.

2.3. PURPOSE

This policy outlines the acceptable use of WUA's Information and Communication Technology (ICT) resources, and the University's expectations of all users, in respect to:

2.3.1. The provision of resources;

2.3.2. Access to resources;

2.3.3. Ethical, responsible and legal use of resources;

2.3.4. Privacy and confidentiality when using resources;

2.3.5. Implications for breaches of this policy.

2.4. SCOPE

This policy applies to all clients of the University ICT resources. It is the individual responsibility of each user of the University's ICT resources to comply with this policy and associated regulations and procedures, as a condition of such an access.

Clients' personal use of University provided ICT services, facilities and devices including where clients' personal devices are used to access the University services.

2.5. PRINCIPLES GUIDING THE POLICY

2.5.1. Leverage on technology

2.5.2. Equitable provision of resources

2.5.3. Ethical conduct and responsible use

2.5.4. Authorised access to resources

2.5.5. Information privacy and confidentiality

2.5.6. Compliance and Monitoring

2.6. POLICY PROVISIONS

2.6.1. POLICY STATEMENT

It is University policy to:

2.6.1.1. Leverage on technology in all business activities

2.6.1.2. Provide affordable and appropriate ICT resources to support business activities

2.6.1.3. Protect information privacy and confidentiality

2.6.1.4. Establish access levels, rights, privileges, obligations, prohibitions and sanctions consistent with the University Information and Communication Policy, aimed at enabling easy access to corporate data and information needed for the different roles of the University community, while assuring the integrity of such data and information and respecting the privacy of individuals.

2.6.1.5. Require all Clients and ICT personnel to always conduct themselves in an ethical, professional and responsible manner

2.6.1.6. Monitor and enforce acceptable use of ICT resources

2.6.2. LEVERAGE ON TECHNOLOGY

All employees and students at the University are encouraged to employ appropriate and affordable technology to optimise individual and University performance in support of the primary activities of the University.

2.6.3. PROVISION OF RESOURCES

2.6.3.1. The University provides significant ICT resources to support the University's primary activities. Primary activities of the University include:

a. Teaching
b. Research
c. Outreach
d. Innovation
e. Industrialisation
f. Institutional communication
g. Administrative functions

2.6.3.2. Activities other than these are secondary. As such, they are not necessarily prohibited or even discouraged. Interference might occur when access to resources is needed for primary activities, or when secondary activities consume too many resources such as memory, storage, bandwidth or support staff time.

2.6.3.3. Should secondary activities interfere in any way with primary activities, they may be terminated immediately whether such activities are explicitly detailed in the ICT policy statements or not. Examples of secondary activities include personal web browsing, social media activities, and reading news

2.6.3.4. The integrity and the security of the University's ICT resources are of critical importance to the University's business continuity and reputation. As such, all resources are managed in accordance with appropriate ICT and organisational standards

2.6.3.5. Unauthorised access to, or interference with, ICT resources may jeopardise the University and is strictly forbidden. This includes the installation of unauthorised software and/or hardware onto University networks or systems, or use of unauthorised games, or other content unrelated to legitimate University purposes via the University network.

2.6.3.6. Staff should use the designated University email system while sending and receiving any communications related to University business and must not use private email accounts for any University related purposes.

2.6.4. ETHICAL CONDUCT AND RESPONSIBLE USE

2.6.4.1. Expectations of acceptable use of ICT resources at WUA are based on ethical considerations in particular respect and promotion of individual rights to privacy, equitable and fair access to resources, intellectual property, and civil rights. Activities which threaten these rights are discouraged and/or prohibited and may be terminated immediately.

2.6.4.2. Clients are expected to exercise responsibility, use resources appropriately and efficiently and respect the rights and privacy of others

2.6.4.3. Clients are expected to demonstrate respect towards all persons. Behaviours such as defamation, discrimination, vilification, bullying and harassment are not only inconsistent with University policies and procedures but may also result in legal action.

2.6.4.4. Clients found to be intentionally accessing, downloading, storing or distributing undesirable content will be subject to disciplinary action for serious misconduct.

2.6.4.5. Clients must operate within the laws of Zimbabwe and the policies and procedures of the University.

2.6.4.6. Clients should limit personal use of ICT resources to incidental, infrequent and brief and should avoid conflicts of interest.

2.6.5. AUTHORISED ACCESS TO RESOURCES

2.6.5.1. The relevant University organisational unit shall determine who has access to ICT resources and the privileges thereof.

2.6.5.2. Clients are responsible for their own accounts and are permitted to access only those resources for which they have been authorised.

2.6.5.3. The sharing of user accounts and passwords, under any circumstances, is explicitly forbidden.

2.6.5.4. No client shall, under any circumstances, take any action that may lead to circumventing or compromising security of the University's ICT resources.

2.6.5.5. The University takes a centralised approach to software asset management. The University will only use a genuine copy of legally acquired software that is configured and used in accordance with the licence terms and conditions as set out by the copyright holder. The making, use and installation of unauthorised or illegal software copies is prohibited.

2.6.5.6. The University deploys a Managed Configuration Management Environment (MCME) to all client computing systems in the designated environment to deliver a stable, supportable and secure platform for University related activity. The Information Technologist is responsible for the signing of software licence agreements, development and implementation of controls, procedures and standards to implement this centrally. Exceptions to the MCME and permission to self-install software are subject to approval by the Information Technologist

2.6.6. INFORMATION PRIVACY AND CONFIDENTIALITY

2.6.6.1. Staff of the University should have no expectation that their WUA email accounts or web-browsing activities, or similar, are personal or private. Staff should be aware that all use of ICT resources may be monitored and recorded, and appropriate actions may be taken if any misuse of these resources is identified.

2.6.6.2. Clients who have authorised access to systems and data containing personal information about staff, students, or other individuals (including, but not limited to, research subjects and patients), or confidential information of the University, must maintain the confidentiality of the information to which they have access.

2.6.7. COMPLIANCE AND MONITORING

2.6.7.1. The University reserves the right to monitor aspects of its information systems and network usage.

2.6.7.2. Any breaches of this policy, by any individual, should be brought to the immediate attention of the Information Technologist. This includes any data breach or attempted breach—whether intentional, accidental, or inadvertent—that results in unauthorized access to, disclosure of, or loss of personal information, as such incidents may require notification to affected individuals and relevant authorities.

2.6.7.3. Breaches of this policy may be referred for investigation as possible misconduct or serious misconduct under relevant University policies and procedures.

2.6.7.4. The University reserves the right to restrict access by a client when faced with evidence of a breach of University policies and/or national law.

2.6.7.5. Where required by law, the University will refer any potential breach to the relevant law enforcement authority and will report any potential breach which may amount to criminal conduct

2.7. ROLES AND RESPONSIBILITIES

Role	Responsibility
Information Technologist	The Information Technologist shall: • Ensure that all appropriate personnel have read, signed, and comply with this policy. • Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy • Implement appropriate monitoring The Information Technologist must: • Develop and maintain written standards and procedures necessary to ensure implementation of and compliance with these policy directives. • Provide appropriate support and guidance to assist employees to fulfil their responsibilities under this directive. • Provide periodic updates to reflect any changes in technology or copyright laws.

	• Change vendor default passwords on all hardware and software before being placed on the network or used for University business. • Perform a system risk assessment annually that identifies threats and vulnerabilities on the University network. • Install the latest security patches for all software and operating systems within 3 weeks of the patch being released by the vendor.

2.8. DOCUMENT VERSION MANAGEMENT AND CONTROL

Document name	ACCEPTABLE USE OF ICT RESOURCES POLICY	 **WUA**
Version reference		
Document owner	ICT	
Superseded Documents		
Approved by		
Date of Approval		
Review date		

3 BRING YOUR OWN DEVICE POLICY

3.1. INTRODUCTION

Bring Your Own Device (BYOD) means accessing Women's University in Africa systems and information through personally owned devices. The policy aims to enable access to the University's resources while maintaining a productive, secure, and efficient business environment.

3.2. INTERPRETATION (DEFINITION OF TERMS)

3.2.1. BYOD (Bring Your Own Device): A policy that allows staff and students to use their personal devices for work-related tasks and accessing company resources.

3.2.3. Device: Any electronic device owned or used by University stakeholders—including employees, students, affiliates, council members, board members, and contractors—such as, but not limited to, smartphones, tablets, laptops, desktop computers, and wearable technology.

3.2.4. Endpoint Security: Measures and protocols implemented to secure access points (endpoints) to a corporate network, including devices used by employees under a BYOD policy.

3.2.5. Mobile Device Management (MDM): Software solutions and protocols used to manage, monitor, and secure mobile devices connected to a corporate network. MDM software may include features such as remote wipe, device encryption, and application management.

3.2.6. Security Controls: Measures put in place to protect corporate data and networks from unauthorized access, data breaches, and other security threats. Security controls may include encryption, access controls, and network monitoring.

3.2.7. Data Loss Prevention (DLP): Strategies and technologies aimed at preventing the unauthorized disclosure or loss of sensitive data. DLP solutions may include encryption, access controls, and content inspection.

3.2.8. Remote Wipe: A security feature that allows administrators to remotely erase data stored on a lost or stolen device to prevent unauthorized access to sensitive information.

3.2.9. Personal Identifiable Information (PII): Any information that can be used to identify an individual, such as name, address, Social Security number, or financial information.

BYOD policies often include guidelines for handling and protecting PII on personal devices.

3.2.10. Compliance: Adherence to relevant laws, regulations, and industry standards governing data privacy, security, and confidentiality.

3.3. PURPOSE

The purpose of this policy is to:

3.3.1. Protect the University's information and physical infrastructure.

3.3.2. Promote responsible use of personal devices for academic and research purposes.

3.3.3. Ensure compliance with relevant laws and University regulations.

3.3.4. Provide guidance on the acceptable use of personal devices in the academic environment.

3.4. SCOPE

This policy applies to all clients who use personal devices to access University resources, including but not limited to Wi-Fi, email, internet, learning management systems, and other information systems. It covers all types of personal devices, including laptops, smartphones, tablets, and any other internet-enabled devices.

3.5. PRINCIPLES GUIDING THE POLICY

3.5.1. All devices connected to the University network are required to adhere to the University's Acceptable Use Policy.

3.5.2. Devices must normally be current on all software updates and security software.

3.5.3. Users are also required to follow the Data Protection Act.

3.5.4. The ICT department may, without notification, prevent or ban any personally owned device in the interest of wider University business

3.6. POLICY PROVISIONS

3.6.1. POLICY STATEMENT

It is University policy to encourage all University Clients, especially students, to use their own devices to access selected ICT services availed by the University to enable timely access to information.

This policy does not replace the obligations of the University to provide computing services and devices for use by students and staff.

3.6.2. POLICY OBJECTIVES

3.6.2.1. Enhance productivity: Facilitate seamless access to academic and administrative resources from personal devices, enabling flexibility and mobility for students and staff.

3.6.2.2. Ensure security and data protection: Implement robust security measures to protect University data accessed or stored on personal devices and mitigate potential security threats.

3.6.2.3. Standardize device management: Define acceptable use policies and compliance requirements for personal devices used for University purposes and implement device management solutions to enforce policy adherence.

3.6.2.4. Safeguard privacy: Protect the privacy of personal data on user devices while clearly delineating between University and personal data.

3.6.2.5. Support diverse device ecosystems: Accommodate a variety of devices and operating systems to cater to user preferences and ensure compatibility of University applications across different platforms.

3.6.3. ALLOWABLE USE

3.6.3.1. Personal devices shall be used for activities that directly or indirectly support the business of Women's University in Africa and for learning, teaching, and research.

3.6.3.2. Clients may use their mobile device to access the following University-owned resources: email, calendars, contacts, documents, etc.

3.6.4. UNALLOWABLE USE

3.6.4.1. Unauthorized access to University systems or data.

3.6.4.2. Engaging in any form of cyberbullying, harassment, or academic dishonesty.

3.6.4.3. Downloading, sharing, or distributing copyrighted materials illegally.

3.6.4.4. Performing any actions that could harm the University's network or other users.

3.6.5. DEVICES AND SUPPORT

3.6.5.1. Smartphones, tablets, and laptop computers are allowable devices.

3.6.5.2. Only connectivity issues are supported by the ICT department; employees and students should contact the device manufacturer, their carrier or authorised dealers for operating system or hardware-related issues.

3.6.5.3. The University takes no responsibility for supporting, maintaining, repairing, insuring or otherwise funding employee or student owned devices, or for any loss or damage, resulting from support and advice provided.

3.6.5.4. Devices may be presented to the ICT department for registration, proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the University network.

3.6.6. DATA STORAGE

3.6.6.1. Users must not save any University-owned data which may be considered personal, sensitive, confidential or of commercial value to personally owned devices.

3.6.6.2. The University provides information systems such as University email, which allow secure access to data using an internet browser. When accessing these systems using a personally owned device, users should ensure that they log out.

3.6.6.3. The University reserves the right to clear data stored on any personally owned device which has been used to access University data. This may also result in the removal of any personal data stored on the device. Users shall be responsible for backup of personal data.

3.6.7. REIMBURSEMENT

3.6.7.1. The University or any of its staff are not liable for loss of or damage to a personal device while the device is on University premises. Clients are encouraged to insure their device.

3.6.7.2. The University will not pay the user an allowance for the use of their own device.

3.6.8. SECURITY

3.6.8.1. Personal devices belonging to authorised users of the network i.e. staff, guests, or students, shall be allowed to connect to network and Wi-Fi resources using authorised domain names and credentials.

3.6.8.2. To prevent unauthorized access on the actual device, devices must be password protected using the features of the device and a strong password is required to access the University network.

3.6.8.3. The device must lock itself with a password or PIN if it is idle for more than five minutes.

3.6.8.4. Employees are automatically prevented from downloading, installing, and using any app that does not appear on the University's list of approved apps.

3.6.8.5. User's access to University data is limited based on user profiles defined by the ICT department and automatically enforced through the Domain Name Services (DNS) Server and Active Directory Services.

3.6.9. RISKS/LIABILITIES/DISCLAIMERS

3.6.9.1. While the University's ICT department will take every precaution to prevent the user's personal data from being lost if it must remotely wipe a device, it is the user's responsibility to take additional precautions, such as backing up.

3.6.9.2. The University reserves the right to inspect the device if it is believed that acceptable use policies have been violated.

3.6.9.3. The University reserves the right to disconnect devices or disable services without notification.

3.6.9.4. The client is expected to always use their devices in an ethical manner and adhere to the University's acceptable use policy as outlined above.

3.6.9.5. The client is liable for all costs associated with their device.

3.6.9.6. The user assumes full liability for risks including, but not limited to, the partial or complete loss of University and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

3.7. ROLES AND RESPONSIBILITIES

Roles	**Responsibility**
Information Technologist	The Information Technologist: i. Shall continually monitor usage of BYOD. ii. May temporarily or permanently halt use of one or more types of BYOD where necessary to protect the University Data & Digital Service. iii. May for the same reason also temporarily or permanently halt use for a specific user or users' group of BYOD.

Clients	Shall ensure that their use of personally owned devices is in line with University requirements to ensure data security and the protection of University owned intellectual property and confidential Information.

3.8. DOCUMENT VERSION MANAGEMENT AND CONTROL

Document name	BRING YOUR OWN DEVICE POLICY	 **WUA**
Version reference		
Document owner	ICT	
Superseded Documents		
Approved by		
Date of Approval		
Review date		

4 ELECTRONIC COMMUNICATIONS POLICY

4.1. INTRODUCTION

This Electronic Communications Policy outlines the acceptable use and guidelines for electronic communications at the University. It aims to ensure that electronic communications are used in a manner that is responsible, respectful, and compliant with applicable laws and University regulations.

4.2. INTERPRETATION (DEFINITION OF TERMS)

4.2.1. Electronic Communications: The transmission of information using electronic technology, including email, instant messaging, social media, and other digital communication tools.

4.2.2. Email System: The platform or service provided by the University for sending, receiving, and managing email communications, typically using University-assigned email addresses.

4.2.3. Instant Messaging (IM): Real-time text communication between two or more users through a software application or mobile device.

4.2.4. Social media: Online platforms and tools that allow users to create, share, and interact with content, including but not limited to Facebook, X (Formerly Twitter), Instagram, LinkedIn, and University-specific social networks.

4.2.5. Official Communication: Messages or information disseminated by the University or its representatives to convey valuable information to students, staff, and other stakeholders.

4.2.6. Confidential Information: Any information that is intended to be kept private and is protected by University policy or law, including personal data, academic records, financial information, and proprietary research.

4.2.7. User Responsibilities: The duties and obligations of individuals using the University's electronic communication tools, including adherence to policy guidelines, maintaining security, and using resources appropriately.

4.2.8. Acceptable Use Policy (AUP): A set of rules and guidelines that define appropriate and acceptable behaviour when using the University's electronic communication systems and resources.

4.2.9. Spam: Unsolicited and often irrelevant or inappropriate messages sent over the internet, typically to many users, for the purposes of advertising, phishing, spreading malware, etc.

4.2.10. Phishing: A cyber-attack that uses fraudulent communication, often email, to trick recipients into divulging sensitive information such as login credentials or financial information.

4.2.11. Malware: Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems, often spread through electronic communications.

4.2.12. Encryption: The process of converting information or data into a code, especially to prevent unauthorized access during transmission.

4.2.13. Data Privacy: The protection of personal and sensitive information from unauthorized access, use, disclosure, modification, or destruction.

4.2.14. Confidentiality: Ensuring that information is accessible only to those authorized to have access and is protected throughout its lifecycle.

4.2.15. Digital Signature: An electronic signature that uses cryptographic techniques to provide authentication of the signer and ensure the integrity of the signed data.

4.2.16. Record Retention: The policies and practices regarding the duration and way electronic communications and related records are stored and maintained by the University.

4.2.17. Monitoring: The practice of observing and recording the activity and content of electronic communications to ensure compliance with University policies and legal requirements.

4.2.18. Compliance: Adherence to University policies, procedures, guidelines, best practice, and laws

4.2.19. User Authentication: The process of verifying the identity of a user accessing the University's electronic communication systems, typically through a combination of a username and password.

4.2.20. Two-Factor Authentication (2FA): An additional security measure that requires not only a username and password but also something that only the user has access to, like a mobile device, to authenticate identity.

4.2.21. Message Archiving: The process of preserving electronic communications for future reference, legal compliance, or organizational needs.

4.2.22. Unauthorized Access: Gaining access to the University's electronic communication systems or information without permission, which is prohibited and subject to disciplinary action.

4.2.23. Remote Access: The ability to access the University's electronic communication systems from a location outside the campus, typically through a secure connection like a VPN.

4.2.24. Data Breach: An incident where confidential, sensitive, or protected information is accessed, disclosed, or used without authorization, potentially leading to loss or harm.

4.2.25. Email Etiquette: The guidelines and best practices for writing and responding to emails, ensuring professional and respectful communication.

4.2.26. Third-Party Services: External services or platforms used by the University to facilitate electronic communications, which must comply with the University's data privacy and security policies.

4.2.27. Digital Communication Tools: Software and applications used for electronic communication, including email clients, messaging apps, video conferencing tools, and social media platforms.

4.2.28. Firewall: A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

4.2.29. Antivirus Software: Programs designed to detect, prevent, and remove malware and other malicious software from computer systems.

4.2.30. Backup: The process of creating copies of data to protect against loss or corruption, ensuring that information can be restored in the event of a failure or breach.

4.2.31. Incident Response: The procedures and actions taken by the University in response to a security incident or data breach, including investigation, mitigation, and notification.

4.2.32. User Training and Awareness: Programs and resources provided by the University to educate users on secure and appropriate use of electronic communication tools and systems.

4.3. PURPOSE

The purposes of this Policy are to:

4.3.1. Establish policy on privacy, confidentiality, and security in electronic communications;

4.3.2. Ensure that University electronic communications resources are used for purposes appropriate to the University's mission;

4.3.3. Inform the University community about the applicability of laws and University policies to electronic communications;

4.3.4. Ensure that electronic communications resources are used in compliance with those laws and University policies; and

4.3.5. Prevent disruptions to and misuse of University electronic communications resources, services, and activities.

4.4. SCOPE

This policy applies to all electronic communications resources owned or managed by WUA including but not limited to:

4.4.1. Email

4.4.2. SMS

4.4.3. Chats

4.4.4. All electronic communications resources provided by the University through contracts and other agreements with the University;

4.4.5. All users and uses of University electronic communications resources;

4.4.6. All University electronic communications records in the possession of University employees or of other users of electronic communications resources

4.5. GUIDING PRINCIPLES

4.5.1. SECURITY

4.5.1.1. Ensure the confidentiality, integrity, and availability of all electronic communications.

4.5.1.2. Implement strong authentication and encryption measures to protect sensitive information.

4.5.2. PRIVACY:

4.5.2.1. Respect the privacy of users while balancing the need for monitoring to ensure policy compliance.

4.5.2.2. Protect personal and sensitive information from unauthorized access and disclosure.

4.5.3. COMPLIANCE:

4.5.3.1. Adhere to all applicable laws and regulations regarding electronic communications and data protection.

4.5.3.2. Ensure compliance with University policies and guidelines.

4.5.4. PROFESSIONALISM:

4.5.4.1. Encourage the use of electronic communication tools in a professional, respectful, and courteous manner.

4.5.4.2. Promote clear, accurate, and concise communication.

4.5.5. ACCESSIBILITY:

4.5.5.1. Ensure that electronic communication tools and platforms are accessible to all users, including those with disabilities.

4.5.5.2. Provide support and resources to help users effectively utilize these tools.

4.5.6. TRANSPARENCY:

4.5.6.1. Clearly communicate the policies, procedures, and guidelines governing electronic communications to all users.

4.5.6.2. Regularly update users on changes to policies and the reasons behind them.

4.5.7. RESPONSIBILITY:

4.5.7.1. Hold users accountable for their actions when using electronic communication tools.

4.5.7.2. Emphasize the importance of responsible use to maintain the integrity of University communications.

4.5.8. EFFICIENCY:

4.5.8.1. Promote the use of electronic communications to enhance productivity and streamline University operations.

4.5.8.2. Encourage the use of appropriate tools and platforms for diverse types of communication.

4.5.9. ETHICAL USE:

4.5.9.1. Foster an ethical environment where electronic communications are used in alignment with the University's values and mission.

4.5.9.2. Prohibit the use of electronic communication tools for illegal, unethical, or harmful activities.

4.5.10. EDUCATION AND TRAINING:

4.5.10.1. Provide ongoing education and training to users on best practices for secure and effective use of electronic communication tools.

4.5.10.2. Offer resources and support to help users stay informed about modern technologies and potential security threats.

4.5.11. MONITORING AND ENFORCEMENT:

4.5.11.1. Implement monitoring mechanisms to ensure compliance with the policy while respecting user privacy.

4.5.11.2. Establish clear procedures for addressing policy violations and enforcing disciplinary actions when necessary.

4.5.12. SUPPORT AND RESOURCES:

4.5.12.1. Ensure the availability of technical support and resources to assist users with electronic communication tools.

4.5.12.2. Provide guidelines and best practices for maintaining the security and functionality of personal devices used for University communications.

4.6. POLICY PROVISIONS

4.6.1. POLICY STATEMENT

It is University policy to facilitate efficient, and effective communication with staff, students, and external stakeholders using approved electronic communication platforms

4.6.2. POLICY OBJECTIVES

4.6.2.1. Ensure Effective Communication

4.6.2.2. Maintain Security and Privacy

4.6.2.3. Promote Appropriate Use

4.6.2.4. Support Academic and Administrative Functions

4.6.2.5. Compliance with Legal and Regulatory Requirements

4.6.2.6. Enhance Operational Efficiency

4.6.2.7. Protect University Reputation

4.6.2.8. Support Incident Response and Management

4.6.3. PRIVACY AND MONITORING

4.6.3.1. Privacy Expectation: While the University respects the privacy of users, it reserves the right to monitor and review electronic communications as necessary to ensure compliance with this policy.

4.6.3.2. Access to Communications: The University may access and disclose the contents of electronic communications for reasons including, but not limited to, legal requests, investigations of misconduct, and system maintenance.

4.6.4. SECURITY

4.6.4.1. Passwords: Users must maintain the confidentiality of their passwords and must not share them with others.

4.6.4.2. Data Protection: Sensitive and confidential information must be protected and shared only with authorized individuals.

4.6.4.3. Reporting Incidents: Any suspected security incidents or breaches must be reported immediately to the University's IT department.

4.6.5. SOCIAL MEDIA

4.6.5.1. Representation: When representing the University on social media, users must adhere to the University's social media guidelines.

4.6.5.2. Personal Use: Personal use of social media must not interfere with work responsibilities and should not misrepresent the user's relationship with the University.

4.6.6. EMAIL

4.6.6.1. Official Communications: Email is an official means of communication at the University. Users are expected to regularly check and respond to emails in a timely manner.

4.6.6.2. Email Signatures: All University-related emails should include the official University email signature.

4.6.7. ELECTRONIC COMMUNICATIONS ALLOWABLE USE

4.6.7.1. Purpose: Electronic communications should primarily be used for educational, research, administrative, and operational purposes that support the University's mission.

4.6.7.2. Compliance: Users must comply with all applicable laws, as well as University policies, including those related to harassment, privacy, and intellectual property.

4.6.7.3. Respect: All communications must be respectful and courteous. Harassment, discrimination, and inappropriate content are prohibited

4.6.8. ELECTRONIC COMMUNICATIONS PROHIBITED USE

4.6.8.1. Illegal Activities: Any use of electronic communications to engage in illegal activities is prohibited.

4.6.8.2. Personal Gain: University resources must not be used for personal financial gain or commercial purposes not related to the University.

4.6.8.3. Unauthorized Access: Accessing or attempting to access another user's account, or confidential information without proper authorization is prohibited.

4.6.8.4. Malicious Activities: Users must not engage in activities that could harm the University's electronic communications systems, such as spreading malware, phishing, or hacking.

4.6.9. ENFORCEMENT

4.6.9.1. Violations: Violations of this policy may result in disciplinary action, including but not limited to, loss of access to electronic communication resources, suspension, or termination of employment or enrolment.

4.6.9.2. Reporting Violations: Suspected violations of this policy should be reported to the University's IT department or appropriate administrative office.

4.7. ROLES AND RESPONSIBILITIES

Roles	**Responsibility**
Information Technologist	The Information Technologist shall: Support Incident Response and Management: i. Establish protocols for responding to electronic communication incidents, such as data breaches or cyber-attacks. ii. Provide mechanisms for reporting and addressing violations of the policy. iii. Adapt to Technological Changes: iv. Continuously update the policy to reflect changes in technology and emerging communication platforms. v. Provide Guidance and Training: vi. Offer guidelines and training to help users understand and effectively use electronic communication tools.

	vii. Encourage responsible and ethical use of electronic communication resources.
Clients	Clients shall i. comply with legal and regulatory requirements: ii. Ensure all electronic communications comply with applicable laws, regulations, and University policies.

4.8. DOCUMENT VERSION MANAGEMENT AND CONTROL

Document Name	ELECTRONIC COMMUNICATIONS POLICY	
Version Reference		
Document Owner	ICT	
Approved by		
Date of Approval		
Review Date		**WUA**

5 INFORMATION SECURITY MANAGEMENT POLICY

5.1. INTRODUCTION

The information security management policy outlines the principles, requirements, and approaches to managing and protecting the University's information assets.

5.2. INTERPRETATION (DEFINITION OF TERMS)

5.2.1. Information Security Management System (ISMS): A systematic approach to managing sensitive University information to ensure its confidentiality, integrity, and availability. It includes policies, procedures, and technical measures.

5.2.2. Confidentiality: Ensuring that information is accessible only to those authorized to have access.

5.2.3. Integrity: Safeguarding the accuracy and completeness of information and processing methods.

5.2.4. Availability: Ensuring that authorized users have access to information and associated assets when required.

5.2.5. Risk Assessment: The process of identifying, analysing, and evaluating risks to information security within the University.

5.2.6. Risk Management: The coordinated activities to direct and control risks related to information security, including risk assessment, risk treatment, risk acceptance, and risk communication.

5.2.7. Asset: Any data, device, or other component of the environment that supports information-related activities. Assets can be tangible (e.g., hardware) or intangible (e.g., data, intellectual property).

5.2.8. Threat: Any circumstance or event with the potential to cause harm to an information asset, including cyber-attacks, natural disasters, and human error.

5.2.9. Vulnerability: A weakness in an information system, process, or control that could be exploited by a threat to cause harm.

5.2.10. Control: Measures that are put in place to manage risks to information security. Controls can be technical (e.g., firewalls, encryption), administrative (e.g., policies, training), or physical (e.g., locks, security guards).

5.2.11. Incident Management: The processes and procedures for detecting, reporting, and responding to information security incidents, including data breaches, cyber-attacks, and system failures.

5.2.12. Data Breach: An incident where information is accessed, disclosed, or used without authorization, potentially compromising its confidentiality, integrity, or availability.

5.2.13. Access Control: The selective restriction of access to information or systems. It involves mechanisms such as user authentication, passwords, and permissions.

5.2.14. Authentication: The process of verifying the identity of a user, device, or other entity in a computer system, often through credentials like passwords, tokens, or biometric data.

5.2.15. Authorization: The process of granting or denying access rights to a user, program, or process.

5.2.16. Encryption: The process of converting information into a code to prevent unauthorized access during storage or transmission.

5.2.17. Firewall: A network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

5.2.18. Antivirus Software: Programs designed to detect, prevent, and remove malware and other malicious software from computer systems.

5.2.19. Patch Management: The process of managing updates for software applications and systems to fix vulnerabilities and improve security.

5.2.20. Security Awareness Training: Educational programs designed to inform University staff, students, and other stakeholders about information security threats and best practices for mitigating them.

5.2.21. Business Continuity Plan (BCP): A strategy that outlines procedures for maintaining business operations in the event of a disaster or significant disruption.

5.2.22. Disaster Recovery Plan (DRP): A set of procedures for recovering IT infrastructure and systems after a disaster has occurred.

5.2.23. Audit: A systematic evaluation of information systems and processes to ensure compliance with security policies and to identify vulnerabilities.

5.2.24. Compliance: Adherence to University policies, procedures, regulations guidelines, best practice, and laws and

5.2.25. Security Policy: A document that outlines the University's approach to managing and protecting information assets, including the rules and practices that all users must follow.

5.2.26. Security Incident: Any event that has the potential to negatively impact the confidentiality, integrity, or availability of information, such as unauthorized access, data breaches, or cyber-attacks.

5.2.27. Personal Data: Information that relates to an identified or identifiable individual, which must be protected according to privacy laws and regulations.

5.2.28. Sensitive Information: Data that requires higher levels of protection due to its nature, including personal data, financial information, and intellectual property.

5.2.29. Third-Party Vendor: An external organization that provides services to the University, which may have access to sensitive information and must comply with the University's security policies.

5.2.30. Intrusion Detection System (IDS): Software or hardware designed to detect unauthorized access or anomalies in network traffic that may indicate a security breach.

5.2.31. Security Assessment: An evaluation of the security posture of an information system or environment to identify vulnerabilities and recommend improvements.

5.2.32. Penetration Testing: A method of evaluating the security of an information system by simulating an attack to identify vulnerabilities.

5.2.33. Governance: The framework of policies, processes, and practices that ensure information security aligns with the University's objectives and compliance requirements.

5.2.34. Security Controls: Safeguards or countermeasures implemented to protect information assets and manage risks, including preventive, detective, and corrective controls.

5.2.35. Acceptable Use Policy (AUP): A set of rules and guidelines that define appropriate and acceptable behaviour when using the University's information systems and resources.

5.2.36. Data Classification: The process of categorizing information based on its sensitivity and the level of protection it requires.

5.2.37. Forensics: The application of scientific methods to collect, analyse, and preserve evidence of security incidents for legal and investigative purposes.

5.3. PURPOSE

This policy provides a framework and mechanisms for ensuring the safety, security, confidentiality, integrity, and availability of information while supporting the University's mission of education, research, innovation, industrialisation, and community service.

5.4. SCOPE

This policy applies to all information assets owned, leased, or otherwise under the custody of the University, including but not limited to electronic data, electronic records, and IT systems. It covers all University staff, students, contractors, and third-party service providers.

5.5. GUIDING PRINCIPLES

The following principles underpin this policy:

5.5.1. Information will be protected in line with all relevant University policies and legislation.

5.5.2. It is the responsibility of all individuals to be mindful of the need for information security across the University and to be aware of and comply with this policy including sub-policies and all current and relevant data protection and Zimbabwe's legislation.

5.5.3. Each information asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset.

5.5.4. All information will be classified according to a level of risk.

5.5.5. Information will be made available solely to those who have a legitimate need for access.

5.5.6. It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification.

5.5.7. The integrity of information will be maintained.

5.5.8. Information will be protected against unauthorised access.

5.6. POLICY PROVISIONS

5.6.1. POLICY STATEMENT

It is the University policy to

5.6.1.1. Protect information assets from unauthorized access, theft, and vandalism.

5.6.1.2. Assure data integrity, confidentiality, and availability

5.6.1.3. Ensure that security measures comply with relevant legal requirements and best practices.

5.6.2. POLICY OBJECTIVES

5.6.2.1. Confidentiality: Ensure that information is accessible only to authorized individuals.

5.6.2.2. Integrity: Safeguard the accuracy and completeness of information and processing methods.

5.6.2.3. Availability: Ensure that information and associated assets are available to authorized users when needed.

5.6.2.4. Compliance: Adhere to applicable laws, regulations, and contractual obligations.

5.6.2.5. Risk Management: Identify, assess, and mitigate information security risks.

5.6.2.6. Continuous Improvement: Regularly review and improve the ISMS to adapt to changing threats and business needs.

5.6.3. RISK ASSESSMENT AND TREATMENT

5.6.3.1. Conduct regular risk assessments to identify and evaluate threats to information security.

5.6.3.2. Develop and implement a risk treatment plan to mitigate identified risks to acceptable levels.

5.6.3.3. Review and update risk assessments periodically or when significant changes occur.

5.6.4. INFORMATION SECURITY CONTROLS

The University will implement and maintain controls in the following areas:

5.6.4.1. Access Control: Ensure only authorized individuals have access to information and systems.

5.6.4.2. Incident Management: Establish procedures for detecting, reporting, and responding to information security incidents.

5.6.4.3. Physical Security: Protect physical locations housing information assets from unauthorized access.

5.6.4.4. Network Security: Safeguard the University's network infrastructure from threats.

5.6.4.5. System Acquisition and Development: Ensure information security is integrated into the design and development of new systems and services.

5.6.5. AWARENESS AND TRAINING

5.6.5.1. Provide regular information security training and awareness programs for all employees and students.

5.6.5.1. Ensure that all users understand their roles and responsibilities in protecting information assets.

5.6.6. INCIDENT MANAGEMENT

5.6.6.1. Establish and maintain an incident response plan to address information security breaches promptly and effectively.

5.6.6.2. Ensure all incidents are logged, investigated, and resolved.

5.6.6.3. Analyse incidents to prevent future occurrences and improve the ISMS.

5.6.7. BUSINESS CONTINUITY AND DISASTER RECOVERY

5.6.7.1. Ensure the availability of information and information systems in the event of a disruption.

5.6.7.2. Business Continuity Plan (BCP): Develop and maintain a BCP to ensure the continuity of critical business operations during and after a disruption.

5.6.7.3. Disaster Recovery Plan (DRP): Establish a DRP to restore critical information systems and data in the event of a disaster.

5.6.7.4. Backup: Define and implement regular backup procedures for critical data and ensure that backups are stored securely and tested regularly.

5.6.7.5. Archiving: Define and implement regular archiving procedures for critical data and ensure that backups are stored securely and tested regularly

5.6.7.6. Plan Testing and Review: Conduct regular testing and review of BCP and DRP to ensure their effectiveness and update them as needed.

5.6.8. DOCUMENTATION AND RECORDS

5.6.8.1. Maintain comprehensive documentation of the ISMS including procedures, and records of decisions.

5.6.8.2. Ensure documentation is accessible to relevant stakeholders and regularly reviewed for accuracy and completeness.

5.6.9. INTERNAL AUDIT AND REVIEW

5.6.9.1. Conduct regular internal audits to evaluate the effectiveness of the ISMS.

5.6.9.2. Review audit findings and implement corrective actions to address any deficiencies.

5.6.9.3. Ensure the ISMS is reviewed by senior management when necessary.

5.6.10. DATA PROTECTION

5.6.10.1. Control Objective: Ensure the protection of personal and sensitive data in compliance with applicable laws and regulations.

5.6.10.2. Data Classification: Classify data based on its sensitivity and criticality to ensure appropriate protection measures are applied.

5.6.10.3. Encryption: Implement encryption to protect data in transit and at rest, especially for sensitive and personal data.

5.6.10.4. Data Handling Procedures: Establish procedures for handling, storing, and disposing of data securely to prevent unauthorized access and data breaches.

5.6.10.5. Data Privacy Compliance: Ensure that data protection practices comply with relevant data protection laws and regulations.

5.6.11. CONTINUOUS IMPROVEMENT

5.6.11.1. Monitor and measure the performance of the ISMS against established objectives and key performance indicators (KPIs).

5.6.11.2. Implement improvements based on audit results, incident analyses, and feedback from stakeholders.

5.6.11.3. Stay informed about emerging information security threats and best practices.

5.6.12. COMPLIANCE AND ENFORCEMENT

5.6.12.1. Ensure compliance with applicable laws, regulations, and contractual requirements related to information security.

5.6.12.2. Enforce adherence to this policy and apply disciplinary actions for violations, up to and including termination of employment or academic enrolment.

5.6.13. ALLOWABLE USE

Users must adhere to the following guidelines to ensure responsible and secure use of University information systems:

5.6.13.1. Educational and Administrative Purposes:

a. Use information systems primarily for University-related educational, research, and administrative activities.

b. Personal use should be incidental and not interfere with University operations or resource availability.

5.6.13.2. Access Control:

a. Use only accounts and access permissions that have been authorized by the University.

b. Keep login credentials confidential and do not share them with others.

c. Report any suspected unauthorized access to the Information Security Office immediately.

5.6.13.3. Data Protection:

a. Handle sensitive and confidential information in accordance with University policies and legal requirements.

b. Use encryption and other security measures to protect data in transit and at rest.

c. Report any data breaches or suspected data breaches immediately.

5.6.13.4. Resource Usage:

a. Use University ICT resources efficiently and responsibly.

b. Avoid activities that consume excessive bandwidth or storage space, such as downloading large files for non-University purposes.

5.6.13.5. Software and Hardware:

a. Install and use only software and hardware that is approved by the University's ICT department.

b. Ensure that all software is properly licenced and up to date with the latest security patches.

5.6.13.6. Network Security:

a. Connect only authorized devices to the University network.

b. Use the University's VPN when accessing the network remotely.

c. Do not attempt to bypass network security controls or create unauthorized network connections.

5.6.13.7. Email and Communication:

a. Use University email and communication tools for official University business.

b. Do not send unsolicited bulk emails (spam) or engage in phishing or other fraudulent activities.

c. Be cautious when opening email attachments or clicking on links from unknown sources.

5.6.13.8. Internet Usage:

a. Access internet resources responsibly and avoid websites that pose security risks.

b. Do not engage in illegal activities, such as downloading copyrighted material without authorization.

5.6.13.9. Incident Reporting:

a. Report any information security incidents, vulnerabilities, or suspicious activities to the Information Security Office promptly.

b. Cooperate with investigations and remedial actions related to information security incidents.

5.6.13.10. Compliance and Monitoring:

a. Comply with all applicable University policies, procedures, and guidelines.

b. Be aware that the University may monitor the use of its information systems to ensure compliance and investigate security incidents.

5.6.14. PROHIBITED USE

Users must not engage in the following activities:

5.6.14.1. Unauthorized Access:

a. Attempt to access information systems, data, or accounts for which they do not have explicit authorization.

b. Use another individual's login credentials without permission.

5.6.14.2. Malicious Activities:

a. Introduce malware, viruses, or other malicious code into the University's information systems.

b. Conduct activities that disrupt or degrade the performance of information systems.

5.6.14.3. Data Misuse:

a. Share, distribute, or disclose sensitive or confidential information without proper authorization.

b. Use information systems for personal gain or to engage in activities that conflict with the University's interests.

5.6.14.4. Intellectual Property Infringement:

a. Violate intellectual property rights by downloading, distributing, or using copyrighted material without proper authorization.

5.6.14.5. Network Abuse:

a. Engage in activities that compromise network security, such as port scanning, network sniffing, or unauthorized network probing.

b. Use the network for activities that violate laws and University regulations.

5.7. ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
Information Technologist	• Oversee the development, implementation, and maintenance of the ISMS. • Ensure that the ISMS supports the University's business and academic objectives. • Report regularly to the University leadership on the status and performance of the ISMS. • Develop and enforce information security policies, standards, and procedures. • Conduct risk assessments and implement risk mitigation strategies. • Coordinate responses to information security incidents and breaches. • Lead information security awareness and training programs. • Ensure compliance with legal, regulatory, and contractual information security requirements. • Conduct regular reviews and audits of the ISMS. • Implement and maintain technical controls to protect the University's information systems. • Ensure that all IT systems are configured securely and updated with the latest patches. • Monitor network and system activity to detect and respond to security threats. • Provide technical support for information security initiatives.
Data Owners	• Classify and manage information assets according to their sensitivity and importance. • Define and enforce access control policies for information assets. • Ensure that information is protected throughout its lifecycle
System Administrators	• Manage and maintain the security of IT systems and applications. • Implement access controls and monitor user activities. • Ensure that systems are regularly backed up and can be restored in case of an incident. • Apply security patches and updates to systems promptly.

	•

5.8. DOCUMENT VERSION MANAGEMENT AND CONTROL

Document Name	INFORMATION SECURITY MANAGEMENT POLICY	 **WUA**
Version Reference		
Document Owner	ICT	
Approved by		
Date of Approval		
Review Date		

6 ICT ASSET MANAGEMENT AND DISPOSAL POLICY

6.1. INTRODUCTION

This policy as read with the information security policy, details the regulatory framework for securing the ICT physical infrastructure of the University.

6.2. INTERPRETATION (DEFINITION OF TERMS)

6.2.1. ICT Assets include equipment and devices that can store information. These include desktop computers, laptops, mobile phones, smart phones, tablets, servers, USB memory sticks and external hard drives.

6.3. PURPOSE

This policy outlines the procedures and responsibilities for managing the Information and Communication Technology (ICT) assets of the University, ensuring their efficient use, maintenance, and security.

6.4. SCOPE

This policy refers to all employees, students, and stakeholders of Women's University in Africa.

6.5. PRINCIPLES GUIDING THE POLICY

The following principles guide the ICT Asset Management Policy to ensure the effective and efficient management of the University's ICT assets:

6.5.1. ACCOUNTABILITY

6.5.1.1. Ownership and Responsibility: Clearly define and assign ownership and responsibility for all ICT assets. Each asset should have a designated custodian responsible for its management and upkeep.

6.5.1.2. Transparency: Maintain transparent records of asset acquisition, usage, maintenance, and disposal. Regular audits should be conducted to ensure the integrity of asset management processes.

6.5.2. EFFICIENCY

6.5.2.1. Optimal Utilization: Ensure that ICT assets are used efficiently to support the University's academic, research, and administrative activities. Avoid duplication of resources and maximize the utilization of existing assets.

6.5.2.2. Cost-Effectiveness: Manage ICT assets in a manner that provides the best value for money. This includes careful planning, procurement, maintenance, and disposal to minimize costs and maximize benefits.

6.5.3. SECURITY

6.5.3.1. Protection of Assets: Implement robust security measures to protect ICT assets from unauthorized access, damage, loss, or theft. This includes both physical security and cybersecurity measures.

6.5.3.2. Data Security: Ensure that data stored on ICT assets is protected in compliance with the University's information security policies and relevant legal and regulatory requirements. Sensitive data must be encrypted and securely erased before asset disposal.

6.5.4. COMPLIANCE

6.5.4.1. Regulatory Adherence: Ensure that the management of ICT assets complies with all relevant laws, regulations, and standards. This includes data protection laws, software licencing agreements, and environmental regulations related to the disposal of electronic waste.

6.5.4.2. Policy Compliance: Adhere to the University's internal policies and procedures related to ICT asset management, including procurement, usage, maintenance, and disposal guidelines.

6.5.5. SUSTAINABILITY

6.5.5.1. Environmental Responsibility: Manage ICT assets in an environmentally sustainable manner. This includes considering energy efficiency in asset procurement, promoting the reuse and recycling of assets, and responsibly disposing of electronic waste.

6.5.5.2. Lifecycle Management: Adopt a lifecycle approach to ICT asset management, encompassing planning, acquisition, deployment, maintenance, and disposal. This ensures that assets are managed from initial procurement through to end-of-life in a sustainable and efficient manner.

6.5.6. STANDARDIZATION

6.5.6.1. Consistent Practices: Establish and maintain standardized procedures for the management of ICT assets. This ensures consistency, efficiency, and reliability in how assets are managed across the University.

6.5.6.2. Technology Standards: Adhere to industry standards and best practices in the selection, implementation, and management of ICT assets to ensure compatibility, security, and efficiency.

6.5.7. CONTINUOUS IMPROVEMENT

6.5.7.1. Regular Review: Periodically review and update the ICT asset management policy and procedures to reflect changes in technology, regulatory requirements, and the University's strategic goals.

6.5.7.2. Feedback and Learning: Encourage feedback from stakeholders and use lessons learned from past experiences to improve asset management practices continuously.

6.5.8. USER EMPOWERMENT

6.5.8.1. Training and Awareness: Provide training and resources to ensure that all users understand their responsibilities in relation to ICT asset management. Empower users with the knowledge to use ICT assets effectively and securely.

6.5.8.2. Support and Assistance: Offer support and assistance to users in managing ICT assets, ensuring they have access to the necessary tools and resources to perform their tasks efficiently.

6.6. POLICY PROVISIONS

6.6.1. POLICY STATEMENT

It is the University policy to:

6.6.1.1. Ensure the effective stewardship of its ICT resources

6.6.1.2. Safeguard its technological investments.

6.6.2. POLICY OBJECTIVES

The objective of this ICT Asset Management Policy is to:

6.6.2.1. Ensure the proper management and utilization of ICT assets.

6.6.2.2. Protect ICT assets from loss, damage, and misuse.

6.6.2.3. Provide guidelines for the acquisition, maintenance, and disposal of ICT assets.

6.6.2.4. Ensure compliance with legal, regulatory, and contractual obligations.

6.6.3. ASSET ACQUISITION

6.6.3.1. Procurement Process

a. All ICT asset acquisitions must follow the University's procurement procedures.

b. The ICT Department must be involved in the procurement process to ensure compatibility and standardization..

6.6.3.2. Asset Registration

a. Newly acquired or donated ICT assets must be tagged with a unique identifier.

b. Detailed records of each asset, including its description, location, assigned user, and maintenance schedule, must be maintained in the ICT asset inventory.

6.6.4. ASSET USAGE

6.6.4.1. Allocation

a. ICT assets must be allocated based on the needs and requirements of the University's departments and users.

b. A formal allocation process must be followed to ensure transparency and accountability.

6.6.4.2. User Responsibilities

a. Users are responsible for the proper use and care of allocated ICT assets.

b. ICT assets must not be used for unauthorized or illegal activities.

c. Users must adhere to the University's policies on acceptable use, data protection, and information security.

6.6.4.3. Remote Access and Distance Learning

a. ICT assets used for distance learning must be configured to ensure secure access to University resources.

b. Users must follow best practices for securing their home networks and devices when accessing University systems remotely.

6.6.5. ASSET MAINTENANCE

6.6.5.1. Routine Maintenance

a. Regular maintenance schedules must be established for all ICT assets.

b. The ICT Department must ensure that all software updates, patches, and security measures are applied promptly.

6.6.5.2. Repairs and Servicing

a. Any issues with ICT assets must be reported to the ICT Department for prompt resolution.

b. Only authorized personnel or service providers may perform repairs or servicing on ICT assets.

6.6.6. ASSET SECURITY

6.6.6.1. Physical Security

a. ICT assets must be physically secured to prevent theft, damage, or unauthorized access.

b. Access to areas containing critical ICT assets (e.g., server rooms) must be restricted to authorized personnel.

6.6.6.2. Data Security

a. All data stored on ICT assets must be backed up regularly and securely.

b. Sensitive information must be encrypted and access-controlled to prevent unauthorized access.

6.6.7. ASSET DISPOSAL

6.6.7.1. Disposal Process

a. ICT assets that are no longer needed, beyond repair or that have reached their end-of-life cycle must be disposed of in accordance with University procedures.

b. The ICT Department must ensure that all data is securely erased from the devices before disposal.

c. Environmentally responsible methods must be used for disposing of electronic waste.

d. Mobile devices shall be disposed of in accordance with finance regulations.

6.6.7.2. Asset Disposal

a. Retired ICT assets must be removed from the ICT asset inventory.

b. Records of the disposal process, including methods and dates, must be maintained for audit purposes.

6.6.8. COMPLIANCE AND AUDIT

6.6.8.1. Regular audits of ICT assets must be conducted to ensure compliance with this policy.

6.6.8.2. Any discrepancies or non-compliance issues must be addressed promptly.

6.6.8.3. The ICT Department must report on the status of ICT asset management to the University administration regularly.

6.6.9. TRAINING AND AWARENESS

6.6.9.1. Regular training programs must be conducted to educate users about their responsibilities regarding ICT asset management.

6.6.9.2. Awareness campaigns must be launched to promote best practices in the use and security of ICT assets.

6.6.10. REVIEW AND UPDATES

6.6.10.1. This policy must be reviewed and updated annually or as necessary to reflect changes in technology, regulations, or University requirements.

6.6.10.2. Suggestions for improvements to this policy are encouraged and can be submitted to the ICT Department.

6.6.11. ENFORCEMENT

6.6.11.1. Violations of this policy may result in disciplinary action, up to and including termination of employment or expulsion from the University.

6.6.11.2. Legal actions may be pursued for violations that contravene local laws and regulations.

6.7. ROLES AND RESPONSIBILITIES

ROLES	RESPONSIBILITIES
Information Technologist	i. Ensure that users acquire ICT assets suitable for intended use with reasonable specifications. ii. Maintain the ICT Asset Register which shall capture details of ICT

	resources as follows: Date of Purchase, iii. Description, iv. Asset Number etc. v. Commissioning, configuration and setting-up of newly acquired hardware.
Users	i. Handling University ICT assets appropriately and in accordance with their classification. ii. Ensuring that ICT assets around them are kept safe and in a sound state. iii. At the end of each day, users must ensure that their computers are properly switched off. iv. Users should immediately report faulty hardware to the ICT Department. v. Users must immediately report in writing the loss or theft of any assigned ICT assets to the office of the Procurement Manager with accompanying police reports, and a copy to the ICT Department vi. Users must ensure that they possess documentation of any ICT assets they move from their original position or remove from campus.
Department Heads and Managers	i. Ensure compliance with the policy within their respective departments ii. Report any issues or breaches related to ICT assets to the ICT Department.

6.8. DOCUMENT VERSION MANAGEMENT AND CONTROL

Document name	ICT ASSET MANAGEMENT AND DISPOSAL POLICY	
Version reference		
Document owner	ICT	
Approved by		
Date of Approval		
Review date		

Document Name

WUA

Version Reference

7 SOFTWARE POLICY

7.1. INTRODUCTION

This policy provides a framework for effective management and utilisation of software in the University.

7.2. INTERPRETATION (DEFINITION OF TERMS)

7.2.1. Software: Any program or application that can be run on a computer system, including operating systems, middleware, and end-user applications.

7.2.2. Licence: A legal agreement that permits the use of software under defined conditions.

7.2.3. ICT Department: The department responsible for managing the University's information and communication technology resources.

7.2.4. User: Any individual authorized to use University IT resources, including students, staff, and contractors.

7.2.5. Vendor: A company or entity that provides software products and services.

7.3. PURPOSE

This policy outlines the regulations on acquisition, responsible use, and effective management of software in the University.

7.4. SCOPE

The policy refers to all software used to support University processes.

7.5. PRINCIPLES GUIDING THE POLICY

7.5.1. All software, including operating systems and applications, must be actively managed.

7.5.2. Legal Compliance: Adhere to all relevant laws and regulations regarding software licencing and intellectual property.

7.5.3. Security: Ensure that all software is secure and does not compromise University data or systems.

7.5.4. Efficiency: Promote the efficient use of software resources to maximize value and minimize waste.

7.5.5. Transparency: Maintain clear and open processes for software acquisition, usage, and disposal.

7.5.6. Accountability: Establish clear roles and responsibilities for managing and using software.

7.6. POLICY PROVISIONS

7.6.1. POLICY STATEMENT

It is University policy to

7.6.1.1. Ensure that all software used in the institution is appropriately licenced, and any unauthorised use or copying of software is prohibited.

7.6.1.2. Conform to software usage according to licencing agreements and general University guidelines.

7.6.1.3. Ensure security and continued functionality of software through regular updates and upgrades.

7.6.1.4. Guarantee that all software purchases are approved by the ICT department for compatibility, security, and compliance with University standards.

7.6.2. POLICY OBJECTIVES

7.6.2.1. Ensure Legal Compliance: Adhere to all relevant software licencing agreements, intellectual property laws, and regulatory requirements.

7.6.2.2. Promote Security: Implement robust measures to safeguard University data and systems from unauthorized access, breaches, and other security threats.

7.6.2.3. Enhance Efficiency: Optimize the use of software resources to maximize value and operational efficiency.

7.6.2.4. Maintain Transparency: Provide clear guidelines and processes for the acquisition, usage, and disposal of software.

7.6.2.5. Uphold Accountability: Define clear roles and responsibilities to ensure proper management and ethical use of software.

7.6.3. SOFTWARE ACQUISITION

7.6.3.1. Approval Process: All software acquisitions must be approved by the ICT Department. Requests should be submitted with a clear justification of need, cost analysis, and compatibility assessment.

7.6.3.2. Licencing Compliance: Ensure all acquired software complies with licencing agreements and intellectual property laws.

7.6.3.3. Vendor Assessment: Evaluate software vendors for reliability, security, support, and compliance with University standards.

7.6.4. SOFTWARE INSTALLATION

7.6.4.1. Authorized Installation: Only authorized personnel may install software on University devices. Unauthorized installation is prohibited.

7.6.4.2. Compliance Check: Verify software licencing and compatibility with existing systems before installation.

7.6.4.3. Security Assessment: Conduct a security assessment for new software to ensure it does not compromise University systems.

7.6.5. SOFTWARE USAGE

7.6.5.1. Licence Adherence: Use software strictly in accordance with its licencing agreement. Do not duplicate or distribute software without proper authorization.

7.6.5.2. User Responsibilities: Users must follow guidelines for the correct and ethical use of software. Misuse can result in disciplinary action.

7.6.5.3. Training: Provide training for staff and students on proper software usage and best practices.

7.6.6. SOFTWARE UPDATES AND MAINTENANCE

7.6.6.1. Regular Updates: Ensure all software is regularly updated to the latest versions to maintain security and functionality.

7.6.6.2. Patch Management: Apply patches and security updates promptly to mitigate vulnerabilities.

7.6.6.3. Support and Maintenance Contracts: Maintain support and maintenance contracts for critical software to ensure timely assistance and updates.

7.6.7. SOFTWARE INVENTORY

7.6.7.1. Inventory Management: Maintain an accurate and up-to-date inventory of all software, including licences, installation locations, and usage.

7.6.7.2. Audit: Conduct regular audits to ensure compliance with software licencing agreements and policy adherence.

7.6.8. SOFTWARE DISPOSAL

7.6.8.1. Decommissioning Process: Follow a standardized process for the decommissioning and disposal of software. Ensure all data is securely erased before disposal.

7.6.8.2. Licence Termination: Terminate or transfer software licences as appropriate upon disposal.

7.6.9. SECURITY AND COMPLIANCE

7.6.9.1. Data Protection: Ensure all software complies with University data protection policies and relevant legislation.

7.6.9.2. Access Control: Implement strict access controls to protect software and associated data from unauthorized access.

7.6.9.3. Incident Response: Develop and implement procedures for responding to software-related security incidents.

7.7. ROLES AND RESPONSIBILITIES

Roles	**Responsibility**
Information Technologist	• Responsible for the authoring and update of this policy. Own procedures regarding software procurement and licence conformity. • Oversight: Oversee the implementation and compliance with this software policy. • Support: Provide support for software installation, updates, and troubleshooting. • Training: Organize training sessions for users on software usage and best practices. • Inventory Management: Maintain and audit the software inventory.
Department Heads	• Approval: Approve software acquisition requests from their respective departments. • Monitoring: Monitor the use of software within their departments to ensure compliance with this policy. •

End-users	• Compliance: Adhere to this policy and use software responsibly and ethically. • Reporting: Report any issues or breaches related to software usage to the ICT Department. • Training: Participate in training sessions provided by the ICT Department. •
Software Vendors:	• Compliance: Ensure that their products comply with legal and University standards. • Support: Provide timely support and updates for their software products.

7.8. DOCUMENT VERSION MANAGEMENT AND CONTROL

Document name	SOFTWARE POLICY	
Version reference		
Document owner	ICT	
Approved by		
Date of Approval		
Review date		

8 ARTIFICIAL INTELLIGENCE (AI) POLICY

8.1. INTRODUCTION

This policy provides guidelines and principles for the responsible development, deployment, and governance of artificial intelligence (AI) technologies within the Women's University in Africa.

8.2. INTERPRETATION (DEFINITION OF TERMS)

8.2.1. **Artificial Intelligence (AI):** Refers to the simulation of human intelligence processes by machines, including learning, reasoning, problem-solving, and decision-making.

8.2.2. **Ethical AI:** Encompasses the development, deployment, and use of AI technologies in a manner consistent with ethical principles, such as transparency, fairness, accountability, and inclusivity.

8.2.3. **Bias:** Systematic and unfair preferences or prejudices in AI algorithms or systems that result in discrimination or inequitable outcomes.

8.2.4. **Inclusivity:** Ensuring that AI technologies are accessible and beneficial to diverse populations, including women, minorities, and marginalized communities.

8.3. PURPOSE

The purpose of this policy is to provide a framework for the ethical and responsible development, deployment, and governance of AI technologies at Women's University in Africa. WUA aims to promote transparency, fairness, accountability, and inclusivity in all AI-related activities, thereby maximizing the positive impact of AI while minimizing potential risks and harm.

8.4. SCOPE

This policy applies to all staff, students, and any entities affiliated with Women's University in Africa.

8.5. PRINCIPLES GUIDING THE POLICY

8.5.1. Transparency: WUA is committed to transparency in all AI-related activities, ensuring clear communication about the capabilities, limitations, and potential impacts of AI systems.

8.5.2. Fairness and Equity: WUA will strive to mitigate bias and discrimination in AI algorithms and applications, promoting fairness, equity, and inclusivity in all aspects of AI development and deployment.

8.5.3. Accountability: WUA will hold individuals and entities accountable for the design, implementation, and outcomes of AI systems, promoting responsible decision-making and adherence to ethical standards.

8.5.4. Privacy and Data Protection: WUA will uphold the highest standards of privacy and data protection, respecting individuals' rights to control their personal data and ensuring compliance with relevant laws and regulations.

8.5.5. Security: WUA will prioritize the security of AI systems and data, implementing robust measures to prevent unauthorized access, misuse, and manipulation of AI technologies.

8.6. POLICY PROVISIONS

8.6.1. POLICY STATEMENT

It is University policy to promote the responsible development, deployment, use and governance of AI technologies in accordance with ethical principles and best practices.

8.6.2. POLICY OBJECTIVES

The objectives of this policy are;

8.6.2.1. To ensure that AI technologies developed and deployed by WUA adhere to ethical guidelines and principles

8.6.2.2. To promote transparency, fairness, and accountability in AI-related activities within the University.

8.6.2.3. To mitigate bias and discrimination in AI algorithms and applications as a way of promoting inclusivity and equity

8.6.2.4. To uphold the highest standards of privacy and data protection in AI research and deployment

8.6.3. ETHICAL AI RESEARCH AND DEVELOPMENT

WUA will support and promote ethical AI research and development practices, including the responsible collection, use, and sharing of data, as well as the design of AI systems that prioritize transparency, fairness, and inclusivity.

8.6.4. AI EDUCATION AND TRAINING

WUA will integrate AI literacy and ethics into its curricula and training programs, providing students, academic and administrative staff with the knowledge, skills, and ethical framework necessary to engage with AI technologies responsibly.

8.6.5. COMMUNITY ENGAGEMENT

WUA will engage with local communities, governments, industry partners, and civil society organizations to foster dialogue, raise awareness, and promote ethical AI practices.

8.6.6. GOVERNANCE AND OVERSIGHT

WUA will establish mechanisms for monitoring and evaluating compliance with this policy, including the establishment of an AI ethics committee or task force responsible for overseeing AI-related activities and providing guidance on ethical issues.

8.6.7. CONTINUOUS IMPROVEMENT

WUA will regularly review and update this policy in response to technological advancements, emerging ethical concerns, and evolving regulatory landscapes, ensuring alignment with the University's mission and values.

8.7. ROLES AND RESPONSIBILITIES

ROLES	RESPONSIBILITIES
Information Technologist	Identifying, evaluating, and recommending appropriate AI tools for use in the University
AI Ethics Committee	Responsible for overseeing AI-related activities, assessing ethical risks, and providing guidance on best practices. i. Reviewing and approving AI research proposals, ensuring compliance with ethical guidelines and regulations.

	ii. Assessing the ethical implications of AI systems and applications developed or deployed by WUA. iii. Providing guidance and recommendations on ethical decision-making and risk mitigation strategies. iv. Regularly reviewing and updating WUA's AI policy in response to technological advancements and emerging ethical concerns.
AI Researchers and Developers	Responsible for conducting ethical research and development, mitigating bias, and ensuring transparency in AI systems. Some detailed responsibilities include; i. Conducting ethical research, including the responsible collection, use, and sharing of data. ii. Designing AI systems that prioritize fairness, transparency, accountability, and inclusivity. iii. Mitigating bias and discrimination in AI algorithms and applications through rigorous testing and validation. iv. Collaborating with the AI Ethics Committee to address ethical concerns and implement ethical guidelines and recommendations.
Faculties	Responsible for integrating AI literacy and ethics into curricula and training programs. i. Incorporating AI-related topics into existing courses across disciplines, providing students with a foundational understanding of AI technologies and their ethical implications. ii. Offering specialized training programs and workshops on AI ethics, bias mitigation, and responsible AI design for students, academic and administrative staff. iii. Encouraging critical thinking and ethical reflection among students, fostering a culture of responsible

	AI usage and development within the University community.
University Administration	Responsible for providing resources, support, and oversight to ensure the effective implementation of the AI policy. Specific tasks include; i. Allocating funding and resources for AI research, education, and infrastructure. ii. Establishing mechanisms for monitoring and evaluating compliance with ethical guidelines and regulations. iii. Supporting the AI Ethics Committee in its oversight role and facilitating communication and collaboration across departments and stakeholders. iv. Promoting a culture of ethical conduct and accountability throughout the University.

8.8. DOCUMENT VERSION MANAGEMENT AND CONTROL

Document Name	ARTIFICIAL INTELLIGENCE (AI) POLICY	
Version Reference		
Document Owner	ICT	
Approved by		
Date of Approval		
Review Date		**WUA**

9 ELECTRONIC LEARNING POLICY

9.1. INTRODUCTION

This policy provides a framework to facilitate the cost-effective improvement of the quality of teaching and learning at WUA through leveraging appropriate technologies.

9.2. INTERPRETATION (DEFINITION OF TERMS)

9.2.1. E-Learning: The delivery of education and training through electronic means, typically using digital technologies such as computers, the internet, and multimedia resources.

9.2.2. Learning Management System (myHope): A software platform used to deliver, manage, and track E-Learning courses and materials, including features for content delivery, student interaction, assessment, and performance tracking.

9.2.3. Online Course: A course in which instruction and learning activities are primarily conducted through digital platforms, such as myHope or video conferencing tools, allowing students to participate remotely.

9.2.4. Blended Learning: An instructional approach that combines traditional face-to-face teaching with online learning activities, offering students a mix of in-person and digital learning experiences.

9.2.5. Synchronous Learning: Learning activities that occur in real-time, where instructors and students interact simultaneously through online platforms such as virtual classrooms or webinars.

9.2.6. Asynchronous Learning: Learning activities that can be accessed and completed by students at their own pace and time, without the need for real-time interaction with instructors or peers.

9.2.7. Digital Content: Educational materials and resources delivered in digital formats, including text, images, audio, video, interactive simulations, and online assessments.

9.2.8. Copyright: Legal rights and protections granted to creators of original works, including digital content used in E-Learning courses. University E-Learning policies may outline copyright guidelines and procedures for obtaining permissions to use copyrighted materials.

9.2.9. Access and Equity: Ensuring that E-Learning courses and materials are accessible to all students, regardless of their geographical location, physical abilities, technological resources, or socioeconomic status.

9.2.10. Data Privacy: The protection of personal and sensitive information collected from students and instructors during E-Learning activities, in compliance with relevant data protection laws and University policies.

9.2.11. Digital Citizenship: The responsible and ethical use of digital technologies and online resources by students, instructors, and other participants in E-Learning environments, including respect for intellectual property rights, privacy, and online conduct.

9.2.12. Assessment and Evaluation: Methods and criteria used to assess student learning and performance in E-Learning courses, including online quizzes, assignments, exams, peer assessments, and instructor feedback.

9.2.13. Technical Support: Resources and assistance provided to students and instructors to troubleshoot technical issues related to E-Learning platforms, software, hardware, and internet connectivity.

9.2.14. Professional Development: Opportunities for academic and administrative staff to enhance their skills and knowledge in E-Learning pedagogy, instructional design, technology integration, and online teaching best practices.

9.2.15. Quality Assurance: Processes and standards used to ensure the effectiveness, relevance, and quality of E-Learning courses and materials, including course design, content development, instructional delivery, and student support services.

9.2.16. Pedagogy: The theory and practice of teaching and learning, including instructional strategies, assessment methods, and curriculum design principles employed to facilitate student learning outcomes.

9.2.17. Andragogy: The theory and practice of teaching and learning principles specifically tailored to adult learners, focusing on self-directed learning, problem-solving, and experiential learning strategies.

9.2.18. Instructional Design: The systematic process of designing, developing, and evaluating educational materials and learning experiences, incorporating principles of learning theory, multimedia design, and technology integration.

9.2.19. Learning Objectives: Clear and measurable statements describing the intended outcomes or goals of a learning activity or course, typically aligned with broader program or institutional learning goals.

9.2.20. Learning Outcomes: Observable and assessable results of student learning, reflecting the knowledge, skills, abilities, and attitudes students are expected to acquire or demonstrate because of their educational experiences.

9.2.21. Course Development: The process of designing and creating instructional materials, activities, and assessments for a specific course, ensuring alignment with learning objectives, pedagogical approaches, and assessment strategies.

9.2.22. Course Delivery: The methods and modalities used to deliver course content and facilitate learning experiences, including face-to-face instruction, online learning platforms, blended learning approaches, and experiential learning opportunities.

9.2.23. Technology Integration: The strategic incorporation of digital technologies and educational tools into teaching and learning activities to enhance engagement, interactivity, and effectiveness of instructional delivery.

9.2.24. Student Support Services: Resources and services provided to students to enhance their academic success and well-being, including tutoring, academic advising, counselling, accessibility services, and technical support for E-Learning platforms.

9.2.25. Educational Research: Scholarly inquiry and investigation into teaching and learning practices, instructional innovations, and student outcomes, conducted to inform evidence-based decision-making and improve educational effectiveness.

9.2.26. Community Engagement: Collaborative partnerships and initiatives between the ICT department, academic staff, students, and external stakeholders to promote lifelong learning, educational equity, and community development through educational outreach programs, service-learning opportunities, and community-based research projects.

9.2.27. E-Learning Platforms: Software systems or platforms used to deliver, manage, and support online learning activities, including learning management systems (myHope), virtual learning environments (VLE), and content management systems (CMS).

9.2.28. Infrastructure: The underlying technological framework and resources supporting the delivery of E-Learning services, including network infrastructure, servers, storage systems, and computing devices.

9.2.29. Internet Connectivity: Access to high-speed internet connections and network services essential for accessing online learning materials, participating in virtual classrooms, and engaging in collaborative E-Learning activities.

9.2.30. Digital Access: The availability of computing devices, software applications, and online resources necessary for students and instructors to access E-Learning platforms and educational materials from any location, on-campus, or off-campus.

9.2.31. Security: Measures and protocols implemented to protect E-Learning platforms, student data, and institutional information from unauthorized access, data breaches, malware attacks, and other cybersecurity threats.

9.2.32. Data Privacy: Policies and procedures governing the collection, storage, processing, and sharing of student and staff data in compliance with privacy regulations and institutional policies.

9.2.33. Software Licencing: Agreements and policies governing the procurement, distribution, and use of software applications and digital tools for E-Learning purposes, ensuring compliance with licencing terms and copyright regulations.

9.2.34. Technical Support: Services and resources provided by the ICT department to troubleshoot technical issues, resolve software or hardware problems, and assist staff, and students in using E-Learning platforms and digital tools effectively.

9.2.35. Training and Capacity Building: Workshops, training sessions, and educational resources offered by the ICT department to build the technological skills and competencies of staff, and students in using E-Learning technologies and digital resources.

9.2.36. Accessibility: The design and implementation of E-Learning platforms and digital content to ensure equitable access for students with disabilities, in compliance with accessibility standards such as the Web Content Accessibility Guidelines (WCAG).

9.2.37. Disaster Recovery and Business Continuity: Plans and procedures developed to maintain the availability and integrity of E-Learning systems and services in the event of hardware failures, natural disasters, or other disruptions to ICT infrastructure.

9.2.38. Policy Compliance: Adherence to relevant laws, regulations, standards, and institutional policies governing the use of ICT resources, E-Learning platforms, and digital technologies in educational settings, including copyright laws, data protection regulations, and accessibility guidelines.

9.3. PURPOSE

The purpose of this policy is to facilitate the cost-effective improvement of the quality of teaching and learning and the envisaged growth of WUA through leveraging appropriate technologies.

9.4. SCOPE

This policy is applicable to all teaching and learning activities including staff development programs.

9.5. PRINCIPLES GUIDING THE POLICY

9.5.1. Access to teaching and learning can be improved through a multimodal approach to the delivery of instruction leveraging on relevant and sustainable technologies.

9.5.2. The success of ICT enabled teaching and learning implementation is anchored on the provision of quality content for online student-centred learning.

9.5.3. The ICT department exists to serve academic staff and students within the institution, collaborating with individuals of diverse backgrounds across the institution and outside ranging from beginners to experts.

9.5.4. The University takes consideration of students as a diverse group constituting various backgrounds and abilities, thereby facilitating the development of practices which encourage inclusive teaching and learning.

9.5.5. WUA recognises the importance of advancing instructional delivery, technology adoption, and learner support guided by an institutionalized learning delivery model.

9.5.6. The University acknowledges the need for public interaction to foster conversation and collaboration among the diverse stakeholders of the University to develop and continually enhance blended learning.

9.5.7. The University emphasizes on evidence-based transformation of teaching and learning and assists at various levels the development of relevant approaches to measure impacts of different initiatives in E-Learning.

9.6. POLICY PROVISIONS

9.6.1. POLICY STATEMENT

It is University policy to improve the quality and availability of teaching and learning by leveraging appropriate technologies.

9.6.2. POLICY OBJECTIVES

9.6.2.1. Define and implement a sustainable and effective E-Learning model

9.6.2.2. Implement a quality assurance framework with associated toolkits and artefacts for monitoring and evaluating implementation of E-Learning.

9.6.2.3. Create institutional capacity for sustainable implementation for effective E-Learning.

9.6.2.4. Promote a culture of inclusivity, innovation, research, and development in E-Learning.

9.6.3. E-Learning STAFFING

9.6.3.1. The University shall develop and implement a staffing structure for the ICT department that will ensure efficiency in the management and support for E-Learning with reference to the following areas:

a. In-depth research into the E-Learning delivery models and analysing emerging trends and/or approaches in this field with a view to applying best international practices.

b. Design, development and implementation of internal E-Learning approaches, internationally benchmarked, which integrate the sustainable use of relevant ICTs in the teaching and learning environment.

c. In line with teaching and learning requirements for E-Learning, identify, test, pilot and implement relevant technologies to support internal E-Learning approaches in collaboration with the ICT department.

d. Facilitate the design and development of supportive systems to sustain the continuous implementation and development of E-Learning.

e. Capacity development for academic staff for effective implementation of the University E-Learning delivery model covering areas which include

i. E-Learning course design and development

ii. Content development for online student-centred learning

iii. Teaching and learning interactions to foster attainment of programme learning outcomes

9.6.4. LEARNER SUPPORT AND GUIDANCE

9.6.4.1. Design and development of programmes on E-Learning as a discipline catering for diverse levels to nurture blended learning culture within the University and the nation.

9.6.4.2. Equipping students with requisite skills to study in an E-Learning environment and continually develop their competencies in engaging with online environments for enhanced learning outcomes.

9.6.4.3. Ensuring general inclusivity in the approaches to teaching and learning in the institution.

9.6.4.4. Facilitating the conceptualization, design, and development of a support framework with auxiliary support material in accessible forms.

9.6.4.5. Providing technical support for technologies or platforms used to effectively implement E-Learning.

9.6.4.6. University-wide leadership and support in the transition to E-Learning delivery, management, and delivery of programmes within WUA.

9.6.4.7. The University shall review promotional criteria to recognise E-Learning activities in the promotion of academic and professional staff.

9.6.4.8. Training in E-Learning shall be a prerequisite for academic staff and those coordinating or managing blended learning programmes to ensure quality delivery.

9.6.5. E-LEARNING MATERIALS AND PROGRAMME DELIVERY

9.6.5.1. All programmes on offer shall have appropriate technology mediated study materials, content, and interactive learning activities, developed prior to delivery.

9.6.5.2. All learning material shall be governed by the house style for online courses The Quality Assurance department in conjunction with the ICT department shall internally accredit online instructional delivery material to guarantee effective delivery.

9.6.5.3. All learning material must be developed in cognisance of the need to ensure inclusive access for individuals of diverse backgrounds ranging from gender, learning styles to the physically impaired.

9.6.5.4. The University shall accommodate modular study and multiple exit avenues in E-Learning programs

9.6.5.5. In recognition of the importance of technology in teaching and learning, the University shall continually develop and upgrade its E-Learning delivery and support models with increasing levels of integration of relevant technologies

9.6.5.6. The University shall promote student-centred support systems and assessment mechanisms leveraging on technology for all programmes.

9.6.6. ACCEPTABLE USE

9.6.6.1. Delivery and access to copyright materials on myHope must comply with the Copyright Law.

9.6.6.2. All users of the myHope must not use the system for purposes other than University-affiliated activities.

9.6.6.3. All users of the myHope are responsible for maintaining the security of usernames, passwords and any other access credentials assigned. Access credentials may not be shared or given to anyone other than the user to whom they were assigned.

9.6.6.4. Access to the myHope courses is granted to registered students and designated staff

9.6.6.5. Illegal content shall be removed the user whose account contains illegal content shall be responsible for the costs if any litigation arises because of the content.

9.7. ROLES AND RESPONSIBILITIES

All individuals and units in the University together with those affiliated or associated with the WUA have a responsibility to adhere to this policy and apply it in their respective roles. The overall responsibilities in this regard are as follows:

ROLE	RESPONSIBILITY
Information Technologist	a. Conduct training needs assessments to identify gaps in skills and competencies necessary for the effective delivery and management of programmes in E-Learning environment. b. Train staff to bridge the gap between the available and the desired staff skills and competencies necessary for the productive rolling out of E-Learning programmes c. Run training and development programmes intended to develop pedagogical capacity in E-Learning d. Implement a staff development program for individuals involved in management, design and development of programmes delivered in an E-Learning context. e. Act as an oversight unit in the development and review of E-Learning programmes

	f. Accredit new/revised curricula and content for E-Learning programmes before approval g. Develop toolkits and guides for monitoring and evaluating the efficacy of projects or initiatives in E-Learning h. Assess and review content and activities for online instructional delivery in programmes against internally established standards and criteria i. Provide support services for staff to aid in the implementation of E-Learning j. Provide oversight in the implementation of curricular and student support services k. Develop innovative approaches to support E-Learning programme delivery l. Carry out research and publication in E-Learning m. Design and develop programmes in E-Learning catering for various levels across the University Represent the University on E-Learning platforms and in organisations outside of WUA n. Establish linkages and partnerships with organisations involved in E-Learning o. l p. Market WUA E-Learning expertise and participate in consultancies and development projects related to blended learning q. Manage E-Learning staff, infrastructure, and resources

	r. Manage and coordinate E-Learning activities in Satellite Campuses s. Equip students with requisite skills to study in an E-Learning environment and continually develop their competencies in engaging with online environments for enhanced learning outcomes. t. Develop and submit proposals to fund or attain grants to support the continued development of E-Learning. u. Identify sponsorship opportunities and engage relevant organisations to support E-Learning initiatives in the University v. Establish policies, processes, and procedures to effectively mainstream E-Learning into programme delivery across the University
The University Teaching and Learning Committee	The role of the University teaching and learning committee is to provide policy and strategic direction to advance teaching and learning through the adoption of relevant and sustainable technological solutions.
Quality Assurance Unit	Assuring the quality of programme delivery and related facets is the responsibility of the Quality Assurance unit. The ICT department shall work directly with the Quality Assurance unit to monitor and evaluate E-Learning programme delivery with benchmarked toolkits and guides to ensure quality learning.
Faculty Deans, Satellite Campus Administrators, Unit/Department Heads	These stakeholders are responsible for the implementation of the E-Learning Policy within their areas of operation. This means putting the policy and its strategies into

	practice; making sure all concerned members of staff are aware of their responsibilities and receive support and training in carrying out these responsibilities; and acting against staff or students who default on their obligations to this policy. a. Review existing programs for delivery through an established internal blended learning delivery model with facilitative support from the ICT Department. b. Initiate the development of innovative programs for online learning delivery in liaison with the ICT department. c. Avail academic staff for capacity development in blended learning pedagogy/andragogy and content design, development and delivery through internal tools and platforms. d. Ensure staff receives appropriate E-Learning training e. With assistance from the ICT Department, conceptualise and develop multimedia and other technology mediated study materials for E-Learning programmes f. With oversight from the ICT Department and support from the office of the Dean of Students provide academic and administrative support to students. g. With oversight from the ICT Department, provide requisite E-Learning materials for access upon registration by students before the start of any semester.

	h. Provide formative and summative student assessments in all programmes
Students and Staff	All students and staff shall participate in orientation workshops to develop their understanding and be equipped with the necessary skills and competencies

9.8. DOCUMENT VERSION MANAGEMENT AND CONTROL

Document Name	ELECTRONIC LEARNING POLICY	
Version Reference		
Document Owner	ICT	
Approved by		
Date of Approval		
Review Date		**WUA**

10 ELECTRONIC RECORDING OF MEETINGS POLICY

10.1. INTRODUCTION

This policy provides a framework for the recording of meeting(s) at WUA.

10.2. INTERPRETATION (DEFINITION OF TERMS)

10.2.1. Meetings: Teaching and learning activities, meetings, telephone calls, discussions, or other conversations at WUA, offsite at University organized events, or via any communication channel such as telephone, SMS, WhatsApp, or video conference (such as Zoom or Microsoft Teams) between members of our community.

10.2.2. Teaching and Learning Activities (TLA(s)): Any formal or informal educational events, sessions, or engagements designed to impart knowledge, skills, or understanding to students, including lectures, seminars, tutorials, workshops, laboratory sessions, field trips, and online activities.

10.2.3. Recording: The act of capturing, storing, or documenting meeting through various means such as audio, video, or written materials.

10.2.4. Educational Material: Any resources, content, or materials used in teaching and learning activities, including lecture slides, handouts, textbooks, multimedia presentations, and online resources.

10.2.5. Consent: Permission granted by participants, including academic and administrative staff, and students, for the recording of academic activities in which they participate. Consent must be obtained explicitly from participants.

10.2.6. Data Protection: The principles, regulations, and guidelines governing the collection, storage, processing, and sharing of personal data, including student information, in compliance with relevant data protection laws.

10.2.7. Confidentiality: The obligation to protect the privacy and confidentiality of student information and academic materials recorded during teaching and learning activities, ensuring that they are only accessed and used for legitimate educational purposes and in accordance with University policies.

10.2.8. Intellectual Property: The legal rights and ownership interests associated with teaching and learning materials, including copyright, trademarks, patents, and other forms of intellectual property protection. Universities may have policies specifying ownership

rights and usage permissions for educational materials created by academic, staff, or students.

10.2.9. Accessibility: The design and provision of teaching and learning materials in formats and modalities that are accessible to students with diverse abilities, disabilities, and learning needs, in compliance with accessibility standards and regulations such as the Web Content Accessibility Guidelines (WCAG).

10.2.10. Retention and Storage: The procedures and protocols for the secure storage, retention, and disposal of recorded teaching and learning materials, ensuring compliance with data protection laws and institutional policies on data management and retention schedules.

10.2.11. Pedagogical Use: The legitimate educational purposes for which recorded teaching and learning materials may be used, including student review, revision, assessment, feedback, research, professional development, and instructional improvement.

10.2.12. Third-party Platforms: External platforms or services used for recording, hosting, or sharing teaching and learning materials, including learning management systems (myHope), video hosting platforms, cloud storage services, and social media platforms. Universities may have policies governing the use of third-party platforms for educational purposes, including data privacy and security considerations.

10.2.13. Compliance: Adherence to relevant laws, regulations, standards, and institutional policies governing the recording, use, and management of teaching and learning activities, including academic integrity policies, copyright laws, data protection regulations, and accessibility guidelines.

10.2.14. Course Team: Refers to lecturers allocated to the course and other selected member(s) of the department from which the course is offered.

10.2.15. Responsible Authority: Meeting chairperson or course team responsible for a meeting.

10.3. PURPOSE

The purpose of this policy is to strike a balance between the legitimate uses of audio and video recordings, and concerns including compliance with the law, privacy, and protection of intellectual property staff, student, and stakeholders.

10.4. SCOPE

This policy applies to all WUA meetings.

10.5. PRINCIPLES GUIDING THE POLICY

10.5.1. Fundamental rights of staff, students and other stakeholders of the University shall be valued and safeguarded.

10.5.2. In line with the Data Protection Law, the University will implement data protection by design and apply data minimisation to the recording of personal data; this means recording only as much personal data as is necessary for the teaching and learning activity

10.5.3. Students should, within reason, be able to access recordings of live teaching and learning activities to support their learning.

10.5.4. Copyright restrictions shall be adhered to in any activity done during a recorded session.

10.5.5. All recorded sessions will comply with accessibility requirements, for example captioning.

10.5.6. All recorded content must be stored on University managed media, used, and disposed of in an appropriate manner, in line with University security and records retention policies.

10.5.7. The University retains the right to review material to verify it complies with policies on appropriate content.

10.5.8. Any concerns relating to course content raised by a student will be discussed with the relevant staff members (e.g. Course Leader).

10.5.9. If the material is found to be inconsistent with relevant law in the locations it is being deployed, the material may be taken down or amended, in discussion with the relevant staff members.

10.5.10. Academic freedom will be protected throughout this process, and such removal, or necessary adaptation of content to reflect local legislation, will not automatically be dealt with as a misconduct disciplinary matter.

10.5.11. Where appropriate, staff will be provided with advice and support on matters relating to different legal frameworks as well as the legal use of 3rd party materials e.g. copyright and intellectual property.

10.6. POLICY PROVISIONS

10.6.1. POLICY STATEMENT

10.6.1.1. It is University policy to promote and/or cause the recording of meetings, the administration, manipulation, and storage of the content thereof.

10.6.2. POLICY OBJECTIVES

The recording of meetings is a valuable resource for students and staff and can be beneficially used:

10.6.2.1. To provide an accessible digital record of a meeting;

10.6.2.2. In aid of minute making;

10.6.2.3. To aid students who have accessibility requirements or educational needs;

10.6.2.4. As an aid for revision or post TLA review;

10.6.2.5. To enable complex ideas/concepts to be reviewed and reflected upon;

10.6.2.6. To support students and staff who may have challenges with the English language.

10.6.3. PROHIBITED ACTIVITIES

10.6.3.1. To comply with the law, promote the freedom to share ideas and to respect the privacy of community members, the secret recording of meetings is prohibited.

10.6.3.2. Employees and students are prohibited from arranging for others to record meetings regardless of whether it is for work, educational or recreational related activities, unless specifically permitted under this policy.

10.6.3.3. Neither can they knowingly receive or download recorded conversations, upload them to the internet, or otherwise share, transmit or publish such recordings except as permitted herein.

10.6.4. RECORDING OF LIVE MEETINGS

10.6.4.1. The decision as to whether a live meeting will be recorded rests with the responsible authority. This decision should be made with reference to:

a. Ensuring that all participants who constitute the meeting have access to relevant opportunities irrespective of whether they are on-site or online.

b. Whether the mode of the meeting is conducive to being recorded.

10.6.4.1. Participants should be notified of this policy and alerted to the use of recording through

a. The Student Handbook and
b. The appropriate programme handbook and any course specific guidance.
c. The Terms of Reference for the meeting
d. Where it is the intention for a live meeting to be recorded, participants should be notified in advance.

10.6.4.2. Participant video and sound should be switched off by default at the start of the session to give opportunity for participants to choose to share their video and sound.

10.6.4.3. In the case of TLAs, there should also be a part of each session which is not recorded so that students can engage and ask questions off the record.

10.6.4.4. Recordings of live meetings should only be created using University approved software.

10.6.4.5. Where a live meeting is provided by a member of University staff, they should initiate the recording.

10.6.4.6. Where a live teaching and learning activity is engaged in collectively by a group of students as part of their coursework or assessment, they should agree in advance who will initiate the recording. It should be stored and shared in keeping with the specifications provided on the course.

10.6.4.7. Where a student individually engages in course work or assessment that requires recording, they should initiate the recording. It should be stored and shared in keeping with the specifications provided on the course.

10.6.4.8. When lecturers provide live teaching and learning activities which will be recorded, they should ensure they have appropriate copyright clearance and include appropriate citations for any material covered by the recording.

10.6.4.9. Recordings might include all or any of the following:
a. The content provided in the session (visual and audio)
b. Discussions in the session (verbal and written)
c. Those present in the session and their participation in the session

10.6.4.10. All participants need to be aware that their contributions to recordings, including chats, are legally discoverable and that everyone should communicate with clarity, professionalism, courtesy, and respect, remembering the University's Values.

10.6.5. NOTIFICATION OF RECORDING AND OPT OUT

10.6.5.1. In advance of each meeting and at the start of the meeting it should be stated by the responsible authority if it is to be recorded. Participants should indicate at this point if they do not wish to be recorded.

10.6.5.2. The responsible authority has the right to apply discretion when recording, and pause or subsequently edit or delete a recording, for example if sensitive material is being covered or if the recording is interfering with interactive teaching.

10.6.5.3. There are situations where all or part of a live meeting should not or cannot be recorded, these include:

a. Where a TLA is delivered in a way that makes recording unsuitable e.g. elevated level of interactivity,

b. Where discussion or activities contain confidential or personal information or are commercially or politically sensitive,

c. Where there may be legal, ethical or privacy reasons for not recording,

d. Where a participant has personal reasons that make it inappropriate for their activity to be recorded,

e. Where the facility to record the activity is not available in the space.

10.6.5.4. The responsible authority is responsible for deciding whether the interests in not recording part or all a live meeting outweigh the interests in recording. They should keep a note of this decision and any relevant information which informed it for future reference.

10.6.5.5. If a participant does not wish to be recorded, they should make this known to the responsible authority at the start of the meeting. Where a participant does not wish to be recorded, they may have the following options open to them:

a. Leave the session and view the recording.

b. Stay in the session but hide their identity and not contribute to discussions (for example, in an on-site meeting this may include moving to be out of sight / sound of the recording equipment, in an online session this may include not using the mic or chat etc.).

c. Ask the responsible authority to switch off the recording temporarily during which they may contribute. This may be appropriate if a participant is happy to be recorded but wishes to share something personal or sensitive which relates to the meeting.

10.6.5.6. If a lecturer does not wish to be recorded, they should work with their Course Team to ensure that material from their TLA is made accessible in other ways.

10.6.5.7. One on one meeting between staff and students are private and confidential and must not be recorded unless there is an exceptional, compelling business need and the explicit consent of both parties.

a. The business need and the consent of both parties must be documented in a written exchange between the parties.

b. If such a recording is made, the staff member is responsible for deleting it as soon as possible and controlling access strictly on a need to see basis.

c. Such recordings must never be uploaded to course sites or other pages that are accessible by people other than the parties to the meeting as this would constitute a serious breach of the University policies.

10.6.6. STORAGE OF LIVE RECORDINGS

10.6.6.1. Recordings of live meetings will be stored as follows:

a. Uploaded on the course page on myHope if it is a TLA. This takes place immediately after the end of the recorded session.

b. MS Teams recordings will be stored on Stream and may be linked to or embedded in the course page on myHope in the event they are part of a TLA.

c. Other lecture recording software on-campus will be stored on SharePoint and may be linked to or embedded in the course page on myHope.

10.6.6.2. Guidance on where and how to store recordings may be updated as technology develops. This will be kept up to date by the ICT department and communicated to staff and students through appropriate training and guidance sites.

10.6.6.3. Live recordings that include student participation or which identify students will only be stored for the academic year of recording plus one further year and six weeks.

10.6.6.4. Pre-recordings or recordings made live that do not include or identify students may be reviewed and re-used by Course Teams, with the agreement of the staff who developed the materials.

10.6.6.5. A meeting participant may request that a recording be made unavailable for any of the following reasons:

a. Considers that defamatory, inaccurate, discriminatory, or inappropriate material is included within a recording,

b. Considers that personal or sensitive material relating to them is included within a recording but which they did not intend to share or are subsequently unhappy sharing.

i. The responsible authority may choose to take an alternative approach to ensuring that such material is not shared e.g. editing it from the recording that is made available to other participants. A copy of the original recording must be kept.

10.6.7. ACCESS TO LIVE RECORDINGS

10.6.7.1. Recordings should normally only be accessible within the context in which they were recorded, by those participants in the meeting, unless agreed otherwise by the responsible authority. Only participants of the meeting or students enrolled in a course in the case of a TLA should have access to the recordings.

10.6.7.2. Where students create a recording for the purposes of group work on a course, they should ensure that all members of the group have access to the recording.

10.6.7.3. Group work recordings should not be made available more widely within the course unless under the direction of the Course Team.

10.6.8. USE OF LIVE RECORDINGS

10.6.8.1. Students may only use a recording for personal use in relation to their studies. Students must destroy any copy of the recording at the end of the academic year.

10.6.8.2. Staff may only use a recording for purposes of providing the course.

10.6.8.3. The University may use a live recording for the purposes of

a. An investigation into alleged misconduct of staff, students, or guests.

b. Aiding minute taking.

c. Keeping a record of an event or meeting.

10.6.8.4. Any unauthorised publication or distribution of a recording (including uploading online, sharing via apps or social media) by students or staff will be considered in breach of this policy and may be subject to disciplinary action.

10.6.9. DISPOSAL OF RECORDINGS

10.6.9.1. Students should not delete any recordings of student-only coursework, group work or assessment activities without explicit permission from the Course Leader.

10.6.9.2. At the end of academic year Course Leaders should review their course content and dispose of all recordings of live teaching and learning activities which contain student participation, or which identify students made during the year.

10.6.9.3. Students, staff, and guests must destroy any copy of the recording at the end of the academic year.

10.6.9.4. Recorded meetings of TLAs stored on cloud platforms shall have an expiry of one (1) year beyond which, they are automatically deleted.

Recordings of formal meetings shall be deleted after minute taking and approval is carried out.

10.6.10. LEGAL BASIS FOR PROCESSING PERSONAL DATA AND INTELLECTUAL PROPERTY RIGHTS

10.6.10.1. By recording meetings, the University is processing personal data under the lawful basis that the processing is necessary to perform a task in the public interest. Where staff or guests need to record their contributions to fulfil their duties, the University is processing this data as necessary to fulfil a contract with the individual. By participating in a live meeting, participants are deemed to understand that

a. the University will record and make the recording available in accordance with this guidance and

b. They agree to give the University the necessary licences to use the recordings for the purpose stated in this policy.

10.6.10.2. Performer rights reside with the staff member delivering the session and other participants, who agree that the University may use their performance for learning and teaching in accordance with this policy. Presenters or participants in a session wishing to assert their (moral) right to be identified as author or performer should do so as part of the recording, for example through including an introductory slide.

10.6.10.3. Any staff, student or guest creating a recording will ensure that it complies with copyright restrictions.

10.6.11. REASONABLE ADJUSTMENTS

10.6.11.1. Where students have permission from the University to record sessions as part of any reasonable adjustments to ensure the accessibility of their studies, such recordings do not fall within the scope of this guidance.

10.6.12. COMMUNICATING THIS POLICY

10.6.12.1. The responsible authority is responsible for ensuring that all participants involved in a meeting are aware of their duties under this policy and receive appropriate training and guidance.

10.6.12.2. Registry is responsible for informing all students enrolled of this policy and their rights and responsibilities through the Student Handbook at point of enrolment.

10.6.13. USE OF RECORDINGS BEYOND THE MEETING

10.6.13.1. Where students have produced work which they wish to share outside of the course, they may do so provided:

a. They have written consent of each student and staff member who are part of the recording

b. They have ensured they have appropriate copyright clearance for any material covered by the recording.

10.7. ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
Information Technologist	Provision services, platforms, and relevant infrastructure to cause the recording, editing, storage and disposal of meeting recording
Data Protection Officer	a. Ensure data protection compliance within an institution and help it to be accountable in this respect. b. Raise awareness of data protection issues and encourage a culture of protection of personal data within an institution. c. Give advice and recommendations to an institution about the interpretation or application of the data protection rules.
Office of the Registrar	a. Registry is responsible for informing all students enrolled of this policy

	and their rights and responsibilities through the Student Declaration at point of enrolment. i. Ensuring this information is included in all programme handbooks.
Quality Assurance Unit	i. Establishing Quality Standards ii. Facilitating the development of Quality Processes and Procedures iii. Conducting Quality Audits and Inspections iv. Performance Monitoring and Reporting
Faculty Deans, Satellite Campus Administrators, Unit/Department Heads	Responsible for ensuring that all staff and contingent workers such as Adjunct Professors and guest presenters involved in teaching and learning activities are aware of their duties under this policy and receive appropriate training and guidance.

10.8. DOCUMENT VERSION MANAGEMENT AND CONTROL

Document Name	ELECTRONIC RECORDING OF MEETINGS POLICY	
Version Reference		
Document Owner	ICT	
Approved by		
Date of Approval		
Review Date		WUA

11 CHANGE MANAGEMENT POLICY

11.1. INTRODUCTION

Change is an inevitable and essential component of growth, especially in dynamic environments as that which exists at the Women's University in Africa. As an institution that foster innovation, knowledge, and development, WUA must continuously evolve to meet the demands of students, staff, and external stakeholders. However, effective change requires careful planning, clear communication, and coordinated implementation to minimize disruption and maximize positive outcomes.

This Change Management Policy is designed to provide a structured framework for managing change initiatives within the University. It aims to ensure that all changes—whether related to academic programs, administrative processes, technology, or organizational structures—are introduced in a systematic and transparent manner. The policy emphasizes collaboration, accountability, and a commitment to maintaining the University's mission while enhancing its ability to adapt to internal and external pressures.

11.2. INTERPRETATION (DEFINITION OF TERMS)

11.2.1. Change management is a collective term for all approaches to prepare, support, and help individuals, teams, and organizations in making organizational change.

11.2.2. Software Development Life Cycle (SDLC) refers to a methodology with clearly defined processes for creating quality software.

11.2.3. Hardware is any element of a computer that is physical. This includes things like monitors, keyboards, and the insides of devices, like microchips and hard drives.

11.2.4. Software is anything that tells hardware what to do and how to do it, including computer programs and apps on your phone.

11.2.5. Database is an organized collection of structured information, or data, typically stored electronically in a computer system. A database is usually controlled by a database management system (DBMS)

11.2.6. Telephony is the engineering & science behind the equipment & systems (including telephones) that are needed to create and maintain a call between subscribers of the system.

11.2.7. Major Change refers to a momentous change that is associated with substantial risk and impact with the potential to disrupt or adversely critical operations of the University.

11.2.8. Minor Change refers to non-trivial changes that rate low on risk and impact.

11.2.9. Standard Changes, like minor changes, are low on risk and impact. However, these are periodic changes with set standard operating procedures built around them.

11.2.10. Emergency Change is an unexpected interruption that calls for a speedy resolution.

11.3. PURPOSE

The purpose of this policy is to establish how changes to any aspect of the institution's systems, methods, processes, or other resources, whether physical or otherwise will be managed. It will define the specific strategies that must be followed to effect and control this change and how to aid stakeholders in adapting to these transitions.

11.4. SCOPE

11.4.1. The scope of this policy applies to all changes to platforms and services provided by the ICT department, with the following primary functional components being covered in the Change Management Process (CMP):

11.4.1.1. SDLC – Changes handled through the formal software development life cycle will be included within the company's change management program.

11.4.1.2. Hardware – Installation, modification, removal, or relocation of computing equipment.

11.4.1.3. Software – Installation, patching, upgrade, or removal of software products including operating systems, access methods, commercial off-the-shelf (COTS) packages, internally developed packages, and utilities.

11.4.1.4. Database – Changes to databases or files such as additions, reorganizations, and major maintenance.

11.4.1.5. Application – Application changes being promoted to production as well as the integration of new application systems and the removal of obsolete elements.

11.4.1.6. Moves, Adds, Changes and Deletes – Changes to system configuration.

11.4.1.7. Scheduled Changes - Requests for creation, deletion, or revision to job schedules, back-up schedules or other regularly scheduled jobs managed by the ICT department.

11.4.1.8. Telephony – Installation, modification, de-installation, or relocation of PBX/VOIP equipment and services.

11.4.1.9. Desktop – Any modification or relocation of desktop equipment and services for users or classroom labs.

11.4.1.10. Generic and Miscellaneous Changes – Any changes that are required to complete tasks associated with normal job requirements.

11.4.1.11. Changes made to non-priority ICT components - such as systems that are not yet in production, development environments or testing environments - are outside the scope of this policy. This also includes changes made within the daily administrative process such as;

a. Password resets
b. User adds/deletes
c. User modifications
d. Adding, deleting or revising security groups
e. Rebooting machines when there is no change to the configuration of the system
f. File permission changes

11.4.1.12. The scope can be modified periodically to include items in the scope of University's overall Change Management process.

11.5. PRINCIPLES GUIDING THE POLICY

11.5.1. While change is inevitable and a frequent necessity, it must be controlled in such a way that all stakeholders benefit positively, that all systems are enhanced and that structures operate smoothly. This policy is therefore guided by the view that:

11.5.3.1. Change is inevitable but can be managed.

11.5.3.2. Stakeholders must be aware of planned changes.

11.5.3.3. All affected individuals must be trained or sensitized in response to planned changes.

11.5.3.4. Change activities must be conducted in harmony with the other.

11.5.3.5. Changes must be designed to improve satisfaction, comfort, efficiency, and welfare.

11.5.3.6. National and professional standards in various sectors must be considered for each change.

11.6. POLICY PROVISIONS

11.6.1. POLICY STATEMENT

11.6.1.1. It is University policy that ALL changes, new services, enhancements or amendments to any platform or service including cloud services go through a change management process.

11.6.2. POLICY OBJECTIVES

The Change Management Policy has the following objectives:

11.6.2.1. To protect the computing environment from uncontrolled changes.

11.6.2.2. To restrict service disruptions caused by necessary changes to low-use hours.

11.6.2.3. To minimize the occurrence of unintended effects during the implementation of necessary changes.

11.6.3. CHANGE MANAGEMENT PROCESS FLOW

11.6.3.1. Request for Change (RFC): Identification of the need for a formal change request

a. A new request for change can be initiated by any user.

b. The need for an ICT change can be the result of an ICT incident or problem, a new system release, or a specific request, including, for example:

i. Commissioning or decommissioning an ICT system or service.

ii. Modifying a system configuration that requires ICT involvement.

iii. Developing, coding, scripting, or programming a system or application.

iv. Patching and updating system firmware, operating system or software.

v. Making bulk changes to systems and data in production, outside of standard business operations or application functionality processes.

vi. Modifying security group, roles and privileges.

vii. Modifying the security configuration of ICT systems, applications and networks.

c. Change requests must be submitted to the ICT department for consideration and approval by the Information Technologist.

11.6.3.2. Change Assessment and Planning

a. Business value, business risk, technical risk, and cost must be assessed as part of a formal review of new change requests, by the requesting University department and the ICT department.

b. The Information Technology must ensure that major changes are communicated to the appropriate stakeholders. This includes, at minimum the:

i. Representation of the department requesting change.

ii. ICT department representation.

iii. Deputy Information Technologist responsible for the team that will implement the change.

iv. Information Technologist or representative.

i. The Change Requestor must provide sufficient information to analyse the change request prior to submitting the change request for approval.

11.6.3.3. Change Approvals

a. Major and Emergency change requests must be formally approved at a meeting of the ICT Department and the requesting department(s).

b. The departments (in a. above) make decision about Major Changes and meet regularly, as required to monitor implementation.

c. The departments make decisions about high-impact Emergency Changes and meet upon request by the Information Technologist.

11.7. ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
Information Technologist	a. Chair the change management meetings, including presentation of the status of all change requests (new, pending, issues, completed) and formal documentation. a. Review change requests, including their potential impacts and level of risk in liaison with requesting departments. b. Provide formal approval to implement change requests. c. Review change progress with respect to the approved schedule, and participate in Post Implementation Reviews. d. Provide recommendations regarding the implementation of changes into production, prioritize change requests, and make decision if any conflict occurs. e. Provide recommendations to improve or update this Policy.

Faculty Deans, Satellite Campus Administrators, Unit/Department Heads	a. Initiates a Request for Change (RFC) with the required details. b. Communicate with business stakeholders to ensure business requirements are met. c. Participate in acceptance testing and post implementation reviews as required. d. Review any problem, issue or need from users that would require a new change request. e. Approve new change requests initiated from users. f. Communicate with the ICT department to submit a new change request.
Students	a. The students provides the input and feedback on the change requirements and expectations, and participates in the change testing and evaluation. b. The students also adapt to the change and adopts the new or modified ICT services and infrastructure.

ROLE

RESPONSIBILITY

11.8. DOCUMENT VERSION MANAGEMENT AND CONTROL

Information Technologist

a. Chair the change management meetings, including presentation of change requests (new, pending, issues, completed).

b. Provide recommendations to improve or update this Policy.

c. Respond to any user requesting an ICT Change.

d. Verify the nature and classification of the request and confirm if a formal change request is necessary.

e. Update the status of the change as required.

Change Advisory Board (CAB)

a. Review change requests, including their potential impacts and level of risk.

b. Provide formal approval to implement change requests.

c. Review change progress with respect to the approved schedule, and participate in Post Implementation Reviews.

d. Provide recommendations regarding the implementation of changes into production,