KAMUZU UNIVERSITY
OF HEALTH SCIENCES

# Electronic Data Repository Policy

**OCTOBER 2023**

| | |
|---|---|
| **Policy Name** | Electronic Data Repository Policy |
| **Policy No.** | PL/C.7C.1 |
| **Effective Date** | |
| **Last Review** | |
| **Next Review** | Every five years |
| **Council Approval Date** | |
| **Stakeholders Subjected to this Policy** | Staff, students, consultants, vendors, contractors and/or any other parties with a business interest with the University. |
| **Responsible Officer(s)** | University Librarian, Registrar, ICT Director, Director for Institute of Postgraduate Studies and Research, University Legal Counsel |
| **Responsible Office(s):** | Vice Chancellor |

## 4. TABLE OF CONTENTS

## 5. FOREWORD

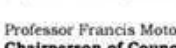
In an era defined by digital transformation and data-driven decision-making, the need for a comprehensive Electronic Data Repository Policy has never been more apparent. Kamuzu University of Health Sciences (KUHeS) recognizes the critical role that data plays in our operations, innovation, and success. As we navigate an increasingly complex data landscape, it is imperative that we establish clear guidelines, best practices, and protocols for managing electronic data repositories.

This Electronic Data Repository Policy represents a pivotal milestone in our commitment to responsible data stewardship. It encapsulates our dedication to safeguarding data integrity, protecting sensitive information, and ensuring data accessibility, all while complying with regulatory requirements and industry standards.

The development of this Policy has been a collaborative effort, drawing on the expertise of professionals across various departments within our organization. It reflects a comprehensive understanding of the challenges and opportunities presented by electronic data repositories, as well as the evolving nature of data management in the digital age.

This Policy serves as a foundational document that guides our data management practices across the all section of our university. It is not static but adaptable, designed to evolve in tandem with technological advancements, emerging risks, and changing regulatory landscapes in agreement with Malawi 2063 vision.

This Policy represents our pledge to uphold these principles, ensuring that our data remains a strategic asset that fuels our growth and innovation.



Professor Francis Moto
**Chairperson of Council**

## 6. PREFACE

In today's digital age, data has emerged as the lifeblood of modern organisations, driving innovation, informing decisions, and fostering growth. As we continue to witness exponential growth in the volume and complexity of electronic data, it becomes increasingly imperative for us to establish a clear and comprehensive framework to govern the management of this valuable asset.

The relentless march of technology has empowered us with remarkable capabilities to collect, store, and analyse data. However, this technological progress also presents us with a unique set of challenges, including data security, privacy concerns, loss of institutional data stored on personal devices of staff when they leave and regulatory requirements. In this dynamic environment, it is our duty to strike a balance between harnessing the potential of data and safeguarding against its inherent risks.

As we embark on this journey of responsible data management, it is crucial to recognize that this Policy is not merely a set of rules and regulations; it reflects our organisation's values and principles. It is a commitment to transparency, accountability, and trust.

As the custodians of data within our organisation, we have a profound responsibility to ensure its proper handling and protection. This Electronic Data Repository Policy represents our collective dedication to fulfilling that responsibility and leveraging data as a strategic asset that propels our organisation into the future.

Professor MacPherson Mallewa
**Vice Chancellor**

## 7. ACKNOWLEDGMENTS

This Policy is the result of collaborations among various players. This work has been made possible by the tireless efforts of the KUHeS family, affiliates, and other stakeholders in the arena.

The task force's dedication to the development of the Policy was admirable. We thank Dr Cecelia Maliwichi Nyirenda and late Mr Gibson Masache from the Research Support Centre under the CHEER Project for their financial assistance in meeting the costs of developing this Policy, as no special funds were set aside for this purpose.

The acknowledgement section would be incomplete unless we mention the staff members who worked tirelessly on this piece of work. Dr Diston Chiweza, Dr Patrick Mapulanga, Mrs Diana Mawindo Chitimbe, and Mr Tobias Makweya from the Library; Mr Chikumbutso Geremu from the ICT Department; and Mr Praise Kafulatira, Archivist from the Malawi Liverpool Wellcome Trust. Mr Yesaya Nyirenda, Data Manager; Mr Amos Msopera, Data Officer; Mrs Atusaye Ngwira, Senior Clinical Research Associate; Mrs Esther Gondwe, Grants Manager; Richard M'madi, Training Coordinator Officer; Mr Peter Mchenga, IT Data Management Unit; Ms Khama Mita, COMREC (now KUREC) Administrator; Mr Andrew Bauleni, Data Coordinator, Malaria Alert Center, Mrs Sthembiso Msisha, and Mrs Gloria Namacha, Administrative Assistant deserve special recognition. Finally, the valuable input of Management and Council in the development of the Policy is greatly appreciated.

## 8. LIST OF ABBREVIATIONS

| | | |
|---|---|---|
| CHEER | : | Capacity Building for Health Profession Education and Research in Malawi |
| DCMI | : | Dublin Core Metadata Initiative |
| KUHeS | : | Kamuzu University of Health Sciences |
| IEC | : | International Electrotechnical Commission |
| ISO | : | International Organisation for Standardisation |
| METS | : | Metadata Encoding and Transmission Standard |
| MOU | : | Memorandum of Understanding |
| SLA | : | Service Level Agreement |
| TR | : | Technical Reports |
| USB | : | Universal Serial Bus |
| EDR | : | Electronic Data Repository |
| EDRs | : | Electronic Data Repository Services |

## 9. DEFINITIONS

| | | |
|---|---|---|
| **Associated materials** | : | Data or files that provide context aid in the interpretation of or are required in the process of rendering and distributing digital content. |
| **Authenticity** | : | A digital record's dependability. This refers to the fact that whatever is being cited is the same as when it was first created unless the accompanying metadata indicates otherwise. |
| **Born-digital** | : | Digital materials are not intended to have an analogue equivalent, either as the source or as a result of conversion to analogue form. |
| **Carrier** | : | A physical item that contains content that has been recorded, encoded, or fixed. This can be saved as analogue or digital data. |
| **Co-master** | : | A preservation master file is the source of the co-master file. Cropping, filtering, and other similar actions can be applied to the co-master. It is usually the source from which access copies are generated, and it may be considered a high-quality access file in and of itself. |
| **Digital content** | : | Text, data, sound recordings, photographs and images, motion pictures, and software are examples of digital items that |

| | | |
|---|---|---|
| | | have been created, published, or distributed. |
| **Digitised content** | : | Content created through the digitisation of an original physical collection item. |
| **File format** | : | A standard method for encoding information for storage in a computer file. |
| **Hosting** | : | Providing a service in which digital content is temporarily in the custody of KUHeS and is responsible for managing and/or preserving this digital content. |
| **Integrity** | : | Data that has remained constant. For instance, data that has gone through a process (such as transmission or storage and retrieval) is identical to how it was before the process began. |
| **Metadata** | : | Information describing important aspects of a 'digital object'. |
| **Migration** | : | The process of moving digital data from one system to another. This may entail exporting from one system and importing it into the new system. |
| **Original** | : | A physical item in a collection, such as a book, manuscript, painting, sculpture, or carrier. The original physical item and physical original are terms that can be used to describe this item. |
| **Preservation action** | : | A specific, defined, and |

| | | |
|---|---|---|
| | | measurable task is performed on a digital file or files to stabilise and/or make them accessible. |
| **Preservation master** | : | Digital content intended for preservation is considered the "master" version of any "digital object's" digital object's intellectual content. |
| **Reformatting** | : | Copying information content from one storage medium to another (media reformatting) or converting one file format to another (file reformatting). |

## 10. BACKGROUND AND SCOPE

The proliferation of data privacy regulations, such as the General Data Protection Regulation (GDPR) and the Malawi Privacy Act, Electronic Transactions and Cyber Security Act necessitates rigorous compliance in data handling. Effective data governance is essential for ensuring data accuracy, consistency, and accountability across the organisation.

This Policy applies to all University employees, contractors, consultants, volunteers, service providers, and vendors who acquire, create, manage, preserve, store, and make available digital content from collections as well as other digital content for which the university is responsible. The Policy also applies to funding organisations, philanthropic organisations, donors, researchers, and all users of the University's digital content.

## 11. RATIONALE FOR THE POLICY

### 11.1 Situation analysis and policy direction

KUHeS, which officially started its operations on 4th May, 2021, does not currently have an EDR policy. Despite this, KUHeS' strength and potential lie in its professional expertise such as; a vibrant team of Health Sciences academics, professional researchers and affiliates, a research support team within the Institute of Postgraduate and Research Support which manages grants and research data, professional ICT experts who manage functional campus-wide area networks and a broad range of ICTs, administrative teams that manage administrative data electronically and manually besides a team of library and information professional which manages rich academic databases for research teaching and learning. This potential has, however, been overshadowed by the lack of a proper EDR policy. This has resulted in irregularities in management of data sources, types, technological infrastructure, compliance and legal requirements that go with this. For example: Databases are managed differently by different sections of the University using different standards and protocols.

There is also no systematic cloud storage management of data that is universal and accessible to all members of KUHeS community. Data files servers are yet to be fully utilised and sensitive data is managed as isolated and disjointed pockets by individuals, or sections of the university. This creates a potential threat of data insecurity and loss.

The EDR policy direction, therefore, seeks to make KUHeS, a Health Sciences University, a centre of excellence in data integrity and management that is compliant to Malawi Agenda 2063 that envisions a Malawi that shall have a health sector with advanced data capturing and management systems to support decision-making and policy formulation.

### 11.2 Justification for the Policy

The rationale for the Electronic Data Repository (EDR) Policy lies in the need to efficiently manage, secure, and maintain electronic data assets within an organisation. An EDR Policy provides a structured framework for handling electronic data, including its creation, storage, access, sharing, retention, and disposal. Some key reasons for implementing an EDR Policy:

#### 11.2.1 Data Governance and Compliance

In today's digital age, organisations collect and process vast amounts of data. Ensuring proper data governance is essential to comply with data protection laws. An EDR Policy outlines guidelines for data handling, usage, and storage that align with legal and regulatory requirements.

#### 11.2.2 Data Security

Electronic data is susceptible to various threats, including unauthorised access, data breaches, and cyber-attacks. An EDR Policy helps define security measures, access controls, encryption protocols, and authentication mechanisms to safeguard sensitive information and prevent data leaks.

### 11.2.3 Data Consistency and Accuracy

A well-structured EDR Policy can establish standards for data input, formatting, and documentation. This ensures that data remains consistent, accurate, and reliable across the organisation, reducing errors and facilitating better decision-making.

### 11.2.4 Efficient Data Management

Effective management of electronic data repositories contributes to operational efficiency by enabling streamlined data access, processing, and storage. A well-defined policy facilitates better resource management, reduces redundancy, and ensures that data are readily available to those who require it. This in turn enhances productivity and supports the institution's overall goals and objectives.

### 11.2.5 Collaboration and Sharing

Data have a lifecycle that includes creation, storage, usage, sharing, and eventual disposal. This policy outlines the best practices for managing each stage of the data lifecycle, ensuring that data are handled appropriately throughout its existence. Proper lifecycle management helps optimise storage resources, reduce costs, and ensure timely and secure disposal of data when it is no longer needed.

### 11.2.6 Disaster Recovery and Business Continuity

Electronic data repositories are susceptible to hardware failures, software glitches, and other technical issues. An EDR Policy outlines backup and disaster recovery strategies to minimise data loss and ensure business continuity in case of unforeseen incidents.

### 11.2.7 Resource Optimisation

Efficient data management reduces the risk of duplicated efforts, unnecessary storage costs, and wasted resources. An EDR Policy can guide the efficient utilisation of storage infrastructure and human resources dedicated to managing electronic data.

### 11.2.8 Auditing and Accountability

An EDR Policy establishes an audit trail for data activities, ensuring accountability for data access, modifications, and sharing. This can be crucial for investigating security breaches, compliance violations, or unauthorised data changes.

### 11.2.9 Adaptation to Technological Changes

The digital landscape is constantly evolving, with new technologies and methodologies emerging regularly. This policy is designed to be flexible and adaptive, allowing for regular updates to address new challenges and opportunities. By staying ahead of the technological trends, we can ensure that our data management practices remain current and effective.

### 11.2.10 Maintaining Stakeholder Trust

Stakeholders, including employees, clients, partners, and the public, place significant trust in their ability to manage their data responsibly. By implementing a robust electronic data repository policy, we demonstrate our commitment to protecting information and upholding ethical standards. This fosters trust and confidence, which are vital for maintaining strong relationships and positive reputations.

### 11.2.11 Compliance with legal and regulatory requirements

Organisations are subject to a myriad of legal and regulatory requirements related to data management, including data privacy laws, industry-specific regulations, and internal governance standards. This policy ensures compliance with these requirements, helping avoid legal penalties, reputational damage, and operational disruptions. It provides a framework for adhering to relevant laws and guidelines, thereby ensuring that our data practices meet the highest compliance standards.

An EDR Policy, therefore, serves as a strategic document that outlines how an organisation will manage electronic data throughout its

lifecycle. By providing guidelines for data governance, security, efficiency, and compliance, the Policy supports the organisation's overall data management objectives and safeguards its valuable electronic information.

## 12. KUHeS VISION

A world-class university and centre of excellence in health education, research, and innovation.

## 13. KUHeS MISSION STATEMENT

To advance knowledge, professional competencies, skills, and innovations in health sciences through high-quality student-centred and innovative education and research that responds to and influences the global/national policy, health, and development needs in an efficient, sustainable, and result-oriented manner.

## 14. AIMS OF THE POLICY

The aim of an Electronic Data Repository Policy in a university is to establish guidelines and procedures for the management, storage, access, and retention of electronic data generated or collected by the university's faculty, staff, and students. This Policy is designed to ensure the proper handling and protection of digital information in compliance with legal, ethical, and security standards.

## 15. OBJECTIVES OF THE POLICY

The objectives of the Policy are to:

a. Ensure the security and privacy of sensitive and confidential information stored in electronic format.
b. Define the conditions under which different groups (faculty, students, researchers, etc.) can access and utilise the electronic data stored in the repository.
c. Ensure the accuracy and reliability of electronic data by outlining procedures for data entry, validation, and verification.

d. Establish guidelines for the retention and deletion of electronic data in alignment with legal and regulatory requirements.
e. Facilitate research and academic collaboration by providing a structured platform for sharing and accessing research datasets, scholarly publications, and other academic resources.
f. Address copyright and intellectual property concerns related to the electronic data stored in the repository.
g. Outline strategies for regular data backups and disaster recovery plans to mitigate the risk of data loss due to hardware failures, natural disasters, or other unforeseen events.
h. Ensure that the electronic data repository policy complies with relevant regulations such as data protection laws, industry standards, and any other legal requirements applicable to the University's jurisdiction.
i. Promote awareness and providing training to university members about the policy's guidelines, procedures, and best practices for managing electronic data effectively and securely.
j. Designate responsible individuals or committees for the oversight and implementation of the Policy.

## 16. POLICY PRIORITY AREAS

### 16.1 Policy Priority Area 1: Classes or Formats of Digital Content to be Preserved

**Policy Issue**: There is need for KUHeS to preserve all classes or formats of Digital Content in order to avoid data loss or data obscurity and abuse by individuals or sections of the University.

**Policy Statement**: KUHeS shall develop clear processes for preserving all formats and classes of digital content in line with related policies such as Records Management Policy.

**Policy Strategies:** KUHeS shall employ the following strategies in order to ensure that classes or formats of Digital Content are preserved:

a. This Policy applies to all preservation master, co-master and 'born-digital original' digital content, associated materials, and associated metadata, in the University's custody. The University shall ensure that its digital contents which falls broadly into six classes as shown in Table 1 below, are considered in the scope of this Policy.

b. If digital content fits in or spans several classes, collaborative and cross-departmental approaches to creating, managing, and preserving digital content shall be adopted.

c. The University shall manage, preserve, store, and provide access to affiliate research data through a Memorandum of Understanding (MOU) and other arrangements.

d. The University shall endeavour to care for third-party digital content and metadata in the same manner as its digital content and metadata.

e. Digital content hosted by the University shall have in place an agreement, contract, or MOU that provides data on hosting arrangements, management, preservation of, and access to digital content with third parties.

f. Agreements, contracts, or MOUs shall indicate service-level agreements regarding hosting, preservation, and access arrangements, including time limits and details regarding the custodial transfer of digital content and metadata when hosting arrangements cease.

**Table 1: Classes or formats of digital content to be preserved**

| Class | Type | Description |
|---|---|---|
| 1 | Born-digital affiliate records | Digital archives of affiliate institutions |
| 2 | Born-digital University records | Selected records of the University |
| 3 | Research outputs | Research data, research publications, digital and digitised theses, scholarly digital editions, supplementary research relating to digitised content and associated materials |
| 4 | Published born-digital content | Web archives, eBooks, born-digital maps, born-digital music, ephemera, published born-digital content on carriers and copies of digital subscription materials (archival and/or access copies, as permitted by agreements) etc. |
| 5 | Digitised content | Digitised image content: Two-dimensional (2D) photography and three-dimensional (3D) imaging etc. Digitised Audio-visual content: Moving images (film and video) and sound recordings etc. |
| 6 | In-house created content | Photography and videography of events and lectures, photos of conservation treatments etc. |

### 16.2 Policy Priority Area 2: Access to the Digital Documents

**Policy Issue**: KUHeS shall ensure that digital content is not obscure to users through limited access rights and poor digital management contracts that prohibit universal access.

**Policy Statement**: It shall be the policy of KUHeS to promote access rights to all deserving stakeholders besides ensuring that all legitimate stakeholders in digital content production have contractual agreements that encourage access to all digital content by authorised clients.

**Policy Strategies:** KUHeS shall employ the following strategies in order to digital documents are widely accessed:

a. Data management rights shall only be accessible to authorised users who have access rights to them. For example:
   a. KUHeS shall ensure that authorised parties have access to digital collections whenever possible, contingent on rights and privacy restrictions clauses.
   b. KUHeS shall safeguard the contractual agreements that researchers shall have with their funders regarding restricted access to data for ethical reasons. In this regard, the policy shall ensure that appropriate data rights management strategies shall allow the encryption of documentation by applying persistent protection to it.

### 16.3 Policy Priority Area 3: Curation Management

**Policy Issue**: KUHeS shall through the EDR policy avoid its past challenges that came with lack of technical specifications, proper procedure, lack of proper description of structural metadata and lack of standards that promote the ever-changing environment for data curation management.

**Policy Statement**: It shall be the policy of KUHeS to promote data curation management standards that are in tandem with policy directions of all related policies such collection management and records management.

**Policy Strategies:** KUHEs shall ensure that good curation management is being implemented by all sections of the university through the following strategies:

a. **Conceptualise:** When new digital objects are created by digitising or reformatting analogy collections or through digital projects, appropriate technical specifications shall be used, long-term storage locations identified, and decisions about access shall be made in advance.

b. **Create:** When digital objects are created or acquired, administrative, descriptive, structural, and technical metadata are created or generated, and stored with the objects.

c. **Appraise and select:** Selection for digital preservation is based on the existing Collection Management Policy and Record Management Policy. Digital content will be assumed to be permanent unless explicitly categorised as temporary via a policy document or written agreement.

d. **Ingest:** Ingest digital objects into the digital repository systems shall follow documented procedures, policies, and legal requirements, including:

    i. Procedures for delivery or transfer.
    ii. File verification, validation, and normalisation.
    iii. Transfer of data and metadata into the approved long-term storage system.

e. **Preservation actions:** A series of actions shall be taken before and during the long-term storage of digital assets to ensure their integrity and authenticity, such as:

   i. Detailed procedures and workflows shall be maintained.
   ii. Potential actions include file format review and migration.

f. **Store:** Digital assets shall be stored and backed up in accordance with standards and best practices. On-site servers will be replicated and backed up to the equipment stored in separate campus buildings. In addition, assets are backed up to the cloud storage.

g. **Access, use, and reuse:** Digital objects shall be accessed by authorised users only:

   i. Some digital objects shall be made publicly available through a designated system.
   ii. Some digital objects shall be made available through a designated system but temporarily restricted or embargoed.
   iii. Some categories of sensitive content may be permanently restricted and never made available through a public-facing system.
   iv. Robust read/write/access controls and authentication procedures shall be used whenever applicable.

h. **Transform:** Digital assets require periodic transformations, such as migration to new software, hardware, or file formats, and metadata enhancement.

### 16.4 Policy Priority Area 4: Security

**Policy Issue**: KUHeS being aware of the challenges of data insecurity through lack of proper backup practices, lack of regular updates and use of ineffective antivirus software, shall prioritise Data Security.

**Policy Statement**: It shall therefore be the policy of KUHeS to promote data security that avoids poor backup practices, lack of software updates and use of inefficient antivirus software. This shall be done in collaboration with the ICT policy.

**Policy Strategies:** KUHEs shall ensure that good data security practices are being implemented by all through the following strategies:

a. Digital document storage systems, backup practices, document retention schedules, and procedures for document creation, management, sharing, and deletion shall be audited regularly to identify security vulnerabilities if any.
b. Data repository software should be regularly updated to keep the software and data with the latest security patches designed to protect it from the most recently discovered threats.
c. Appropriate antiviral software shall be procured and installed to detect, prevent, and act against malicious software in the data repository, including viruses.

### 16.5 Policy Priority Area 5: Data Sharing

**Policy Issue**: KUHeS being aware of challenges that emerge during improper data sharing practices such as mismanagement or abuse of human subjects data, non-adherence to the official restricted period of data, lack of consultation with Principal Investigators who are primary owners of data and lack of use of formal requests.

**Policy Statement**: It shall therefore be the policy of KUHeS to promote data sharing that complies with all regulations that are safeguarded by KUHeS Intellectual Property, Communications and Intellectual property policies and other related policies in order to avoid any form of data abuse that comes with improper sharing.

**Policy Strategies:** KUHEs shall ensure that good data sharing practices are being implemented by all through the following strategies:

a. Data derived from human subject research shall require special ethical considerations pertaining to confidentiality and consent.
b. Before data is made available for sharing, primary research teams must have exclusive use of it for an agreed-upon research use period which shall be determined by the key stakeholders determining the data
c. Data may be made available sooner at the discretion of the Principal Investigator if it does not conflict with the project's publication plans.
d. Requests for data sharing must be written using the appropriate Data Access Form.
e. Data shall be anonymised before release for sharing with all personally identifiable information removed.

### 16.6 Policy Priority Area 6: Standards

**Policy Issue**: KUHeS, desirous to be a world class University that is a centre of excellence, is aware of problems arising from lack of standards in Data Repositories Management which hinder the very access to data that was supposed to be promoted.

**Policy Statement**: It shall therefore be the policy of KUHeS to enforce the adherence to local and international standards throughout the life cycle of data besides promotion of compliance to operational standards.

**Policy Strategies:** KUHeS shall support the management and preservation of digital content, the University aims to comply with international standards, specifications, and local regulations relevant to digital data management. The Policy shall be guided by the following standards:

### 16.6.1 Metadata standards and specifications

To establish a common understanding of the meaning of the data in the repository, as well as to ensure proper use of data standards, we shall comply with the following:

a. Dublin Core Metadata Initiative (DCMI) Specifications.
b. METS Metadata Encoding and Transmission Standard.
c. PREMIS Data Dictionary for Preservation Metadata, Version 3.0.

### 16.6.2 Operational standards

To provide a general interpretation of the data by its owners and users and a common understanding of the data, the following standards shall be adopted:

a. ISO 14721:2012 Space data and information transfer systems – Open Archival Information System (OAIS) – Reference Model
b. ISO 31000: 2009 Risk management – principles and guidelines
c. ISO/IEC 27002:2013 – Code of practice for information security controls

### 16.6.3 Technical standards

To establish uniform technical criteria, methods, processes, and practices for the data, the following applied:

a. BS ISO 19005-1:2005 Document management. Digital document file format for long-term preservation.
b. ISO 16175:2011 Information and documentation – Principles and functional requirements for records in digital office environments.
c. ISO 19262:2015 Photography – Archiving Systems – Vocabulary.

d. ISO/IEC 15408 Information technology – Security techniques – Evaluation criteria for IT security.
e. ISO/TR 18492:2005 Long-term preservation of digital document-based information.
f. ICH-GCP E6-R1 International Conference on Harmonisation Good Clinical Practice.

16.6.4 Related Legislation

All Acts and regulations in Malawi related to Electronic Data Repository shall be complied with including the following.

a. Copyright Act of 2017.
b. Malawi Agenda 2063.
c. Access to Information Act of 2017.
d. Official Secrecy Act of 1913.
e. Science and Technology Act 2003.
f. Communications Act of 2016
g. Data Protection Act of 2024

## 17. GUIDING PRINCIPLES

The guiding principles of an Electronic Data Repository Policy in a university are foundational concepts and values that drive the development, implementation, and maintenance of the Policy. These principles help ensure that the Policy aligns with the university's mission, goals, and values while promoting responsible and effective management of electronic data. The following are key guiding principles for the Policy.

### 17.1 Data Security and Privacy

The Policy prioritises the security and privacy of electronic data by implementing appropriate measures to safeguard against unauthorised access, breaches, and data loss. It also ensures compliance with relevant data protection regulations and best practices.

### 17.2 Transparency

The Policy shall maintain transparency in data management practices by communicating to users the purposes for which their data shall be collected, stored, and accessed within the repository. It shall provide information on data handling procedures and user rights.

### 17.3 Data Integrity and Accuracy

The Policy shall emphasise the importance of maintaining accurate and reliable electronic data. These shall be archived by protocols for data validation, verification, and quality control are ensured and the credibility of information stored in the repository is maintained.

### 17.4 Access and Sharing

The Policy shall promote open access to electronic data while respecting intellectual property rights and confidentiality agreements. Access and sharing enable collaboration and knowledge sharing among researchers, students, and faculty members by defining appropriate access levels and sharing mechanisms.

### 17.5 Compliance

The Policy shall adhere to relevant legal, regulatory, and ethical standards in data management and storage. KUHeS shall ensure that the Policy aligns with data protection laws, copyright regulations, and other applicable guidelines.

### 17.6 Ownership and Attribution

The Policy clarifies ownership rights and attribution for electronic data stored in the repository. The Policy shall recognise authorship, intellectual property, and credit for different types of contributions.

### 17.7 Retention and Deletion

The Policy establishes guidelines for the retention and deletion of electronic data to prevent the accumulation of unnecessary or outdated information. The purpose is to ensure compliance with legal requirements and data protection principles.

### 17.8 Responsibility and Accountability

The Policy shall assign roles and responsibilities for the proper implementation and oversight of the Policy. Only designated individuals or committees shall be responsible for data governance, security, and compliance.

### 17.9 User Education

The Policy shall promote awareness and understanding of the policy among all users of the repository. KUHeS shall offer training and resources to educate users about data management best practices, security measures, and their rights and responsibilities.

### 17.10 Adaptability

The Policy shall be adaptable to technological advancements and changing institutional needs. KUHeS shall regularly review and update the Policy to address emerging challenges and opportunities in data management.

### 17.11 Ethical Considerations

The Policy shall uphold ethical principles in the collection, storage, and use of electronic data. KUHeS shall respect participants' rights, consent, and confidentiality when dealing with sensitive information.

### 17.12 Collaboration and Interdisciplinarity

The Policy shall encourage interdisciplinary collaboration by facilitating the sharing of electronic data across different departments, research areas, and academic units within the university.

### 17.13 Sustainability

The Policy seeks to implement sustainable data management practices that consider long-term data preservation, storage costs, and environmental considerations.

## 18. ROLES AND RESPONSIBILITIES

### 18.1 Directors, Administrators and Heads of Unit

The Director/Administrator/Heads of a unit of an established university entity shall be responsible for:

a. Ensuring that Data Repository Policy and Guidelines are effectively followed across the entity.
b. Driving data repository policy advocacy across the University.
c. Developing strategic data repository collaborations and partnerships across the University.
d. Overseeing the Policy's implementation.
e. Ensuring that the Policy conforms to the university's mission and core values, legislative, funding compliance, and other compliance requirements.
f. Supporting all aspects of acquisition, creation, management, and preservation of digital content and processes, including data-preservation efforts.
g. Ensuring adequate staffing levels is necessary to support data acquisition, creation, and preservation efforts.

h. Ensuring professional development opportunities are provided to the staff responsible for the acquisition, creation, management, and preservation of digital content.
i. Securing funding and allocating resources to deliver a robust and long-term funding model for data preservation.
j. Overseeing the integration of big data repositories into research projects.
k. Supporting relevant activities regarding specific policy implementation.
l. Ensuring that vital official data or documents are not hoarded by individuals.

### 18.2 Departmental/Sectional Officers

The interpretation of the data by its owners and users, and a common understanding of the data, departmental/sectional officers, line managers, and managers of various university teams are responsible for the following:

a. Communicating this Policy effectively to all University staff.

b. Managing processes and workflows are relevant to this Policy.

c. Providing support and systems to support processes associated with acquiring, creating, managing, preserving, and providing access to digital content.

d. Ensuring that staff responsible for acquiring, creating, managing, and preserving digital content are provided with professional development opportunities so that they can fulfil the requirements of their job roles.

e. Ensuring that other staff who use digital content are provided with adequate training and/or guidance, as appropriate.

f. Ensuring work practices comply with this Policy.

### 18.3 University Stakeholders

University stakeholders, contractors, consultants, volunteers, interns, service providers, and vendors shall be responsible for the following:

a. Understanding and complying with this Policy.
b. Seeking out professional development opportunities to meet the demands of their job roles.

### 18.4 Affiliates, and researchers

a. Affiliates and researchers shall be alerted of the digital content they have transferred to the repository's custody as managed and preserved.
b. Researchers who provide digital content to the university shall endeavour to deliver the highest possible quality of digital content that is available or can be created.

## 19. MONITORING AND EVALUATION

The Research Support Centre shall be responsible for monitoring and evaluating this Policy as follows:

a. Developing Guidelines for the Policy
b. Developing Standard Operating Procedures

## 20. FINANCIAL IMPLICATIONS

Successful implementation of this Policy requires a commitment of resources towards the structure, procedure, and interventions. More precisely, the University shall budget for and allocate resources towards:

a. EDR implementation generates cost savings by reducing physical storage costs and streamlining document-management processes.
b. Improved efficiency through EDRs saves time and resources, maximising employee output, and reducing operational delays.
c. Robust security measures for EDRs protect against data breaches, avoiding potential financial losses from fines, legal consequences, and reputation damage.

d. Culprits of data breach regulations are subjected to the KUHeS disciplinary procedures and where applicable, these are fined accordingly.
e. EDRs help organisations comply with regulations and mitigate the financial risks associated with non-compliance and penalties some of which are fines that are determined from time to time.
f. The scalability of EDRs allows for flexible data storage and management, reducing capital expenditures, and facilitating adaptation to changing business needs.
g. Integrating EDRs with existing systems and services incurs costs, but can streamline workflows, improve data accuracy, and enhance decision-making.
h. Resource allocation for training in EDR processes, tools, and security, along with on-going support and maintenance costs, are important financial considerations.
i. KUHeS ensures that the EDR operations receive annual budgetary support in order to ensure that its operations are efficient.
j. KUHeS reserves the right to charge access fees to data in its EDRs, provided that these are compliant to all prevailing regulations and ethical standards.