Policy Category	**Data Management Policies**
Policy Title	**Data Protection Policy**
Policy Number	**UNILIL/DMP/0001**
Policy Holder	**Data Management Unit**
Approving Authority	**Governing Council**
Approval Year	**2022**
Review Date	**2024**

1. INTRODUCTION

The University of Lilongwe recognizes the importance of protecting personal data and is committed to processing it responsibly and in compliance with applicable data protection laws and regulations in Malawi and internationally recognized standards.

This Data Protection Policy establishes a framework for ensuring that personal data is collected, stored, processed, and shared in accordance with legal requirements and best practices, while supporting the University's core functions of teaching, research, and community service.

2. PURPOSE AND SCOPE

2.1 Purpose

This policy aims to ensure that:
- Personal data is processed lawfully, fairly, and transparently
- The rights of data subjects are respected and protected
- Risks of data breaches and unauthorized data processing are minimized
- Staff and students understand their responsibilities regarding data protection
- The University complies with relevant data protection legislation

2.2 Scope

This policy applies to:
- All personal data processed by the University of Lilongwe
- All staff (academic, administrative, and support), students, contractors, and third parties processing data on behalf of the University
- All locations from which University personal data is accessed, including home use and remote sites
- All forms of data, whether electronic, paper-based, or any other format

3. DEFINITIONS

For the purposes of this policy, the following definitions apply:

3.1 Personal Data
Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier.

3.2 Sensitive Personal Data (Special Categories of Data)
Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, sex life, or sexual orientation.

3.3 Processing
Any operation or set of operations performed on personal data, including collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure, or destruction.

3.4 Data Controller
The entity that determines the purposes and means of processing personal data. For the purposes of this policy, the University of Lilongwe is the data controller.

3.5 Data Processor
A person or entity that processes personal data on behalf of the data controller.

3.6 Data Subject
The identified or identifiable individual to whom personal data relates.

3.7 Data Protection Officer (DPO)
The designated individual responsible for overseeing the University's data protection strategy and implementation.

3.8 Data Breach
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

4. DATA PROTECTION PRINCIPLES

The University of Lilongwe adheres to the following data protection principles:

4.1 Lawfulness, Fairness, and Transparency
Personal data shall be processed lawfully, fairly, and in a transparent manner in relation to the data subject.

4.2 Purpose Limitation
Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

4.3 Data Minimization
Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

4.4 Accuracy
Personal data shall be accurate and, where necessary, kept up to date; reasonable steps must be taken to ensure that inaccurate personal data is erased or rectified without delay.

4.5 Storage Limitation
Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

4.6 Integrity and Confidentiality
Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

4.7 Accountability
The University shall be responsible for, and be able to demonstrate compliance with, these principles.

5. LEGAL BASIS FOR PROCESSING

5.1 Legal Grounds
The University will only process personal data where it has a lawful basis for doing so. The lawful bases include:

- Consent of the data subject
- Necessity for the performance of a contract
- Compliance with a legal obligation
- Protection of vital interests of the data subject or another person
- Performance of a task carried out in the public interest
- Legitimate interests pursued by the University or a third party

5.2 Consent
Where consent is used as the legal basis for processing:
- It must be freely given, specific, informed, and unambiguous
- It must be as easy to withdraw consent as to give it
- Records of consent must be maintained

- For children under 16, consent must be obtained from a parent or guardian

5.3 Legitimate Interests
Where legitimate interests are used as the basis for processing:

- A legitimate interests assessment must be conducted
- The interests of the University must be balanced against the rights and freedoms of data subjects
- Data subjects must be informed of the legitimate interests being relied upon

5.4 Special Categories of Data
Processing of sensitive personal data requires additional safeguards and may only be carried out:
- With explicit consent of the data subject
- To protect vital interests where the data subject is physically or legally incapable of giving consent
- For employment, social security, and social protection law purposes
- For substantial public interest reasons
- For preventive or occupational medicine, assessment of working capacity, medical diagnosis, provision of health or social care
- For public health purposes
- For archiving, research, and statistical purposes

6. DATA SUBJECT RIGHTS
The University recognizes and will facilitate the following rights of data subjects:
6.1 Right to Information
Data subjects have the right to be informed about the collection and use of their personal data, including:
- The purposes for processing their personal data
- The retention periods for that personal data
- Who it will be shared with

6.2 Right of Access
Data subjects have the right to request access to their personal data and supplementary information.

6.3 Right to Rectification
Data subjects have the right to have inaccurate personal data rectified or completed if it is incomplete.

6.4 Right to Erasure (Right to be Forgotten)
Data subjects have the right to request the deletion or removal of personal data in specific circumstances.

6.5 Right to Restrict Processing
Data subjects have the right to request the restriction or suppression of their personal data in certain circumstances.

6.6 Right to Data Portability
Data subjects have the right to obtain and reuse their personal data for their own purposes across different services.

6.7 Right to Object
Data subjects have the right to object to processing based on legitimate interests, direct marketing, and processing for research or statistical purposes.

6.8 Rights Related to Automated Decision Making and Profiling
Data subjects have rights related to automated decision making and profiling, including the right not to be subject to a decision based solely on automated processing.

6.9 Handling Data Subject Requests
- Requests must be responded to without undue delay and within one month
- Extensions of up to two additional months may be possible for complex requests
- Identity verification procedures must be followed before responding to requests
- No fee will be charged for processing requests unless they are manifestly unfounded or excessive

7. DATA COLLECTION AND PROCESSING

7.1 Privacy Notices
When collecting personal data, the University shall provide data subjects with information including:
- The identity and contact details of the University
- The contact details of the Data Protection Officer
- The purposes and legal basis for processing
- Recipients or categories of recipients of the personal data
- Retention periods
- Data subject rights
- The right to withdraw consent (if applicable)
- The right to lodge a complaint
- Whether the provision of personal data is a statutory or contractual requirement
- Any automated decision-making processes

7.2 Data Collection Methods
Personal data shall be collected by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

7.3 Data Quality
The University shall take reasonable steps to ensure personal data is accurate, complete, and kept up-to-date.

7.4 Data Minimization
Only personal data that is necessary for the specific purpose shall be collected and processed.

7.5 Privacy by Design and Default
- Privacy by design shall be applied to all projects involving personal data
- Data protection impact assessments shall be conducted for high-risk processing activities
- Systems and processes shall be designed to protect data by default

8. DATA SECURITY

8.1 Technical and Organizational Measures
The University shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including:
- Encryption of personal data where appropriate
- Ability to ensure ongoing confidentiality, integrity, availability, and resilience of processing systems
- Regular testing and evaluation of security measures
- User access controls and authentication
- Physical security measures
- Network security

8.2 Access Controls
- Access to personal data shall be limited to authorized personnel with a legitimate need
- Access rights shall be reviewed regularly
- Authentication mechanisms shall be implemented
- Passwords must meet complexity requirements and be changed regularly

8.3 Device Security
- All devices used to access University data must be secured with appropriate measures
- Mobile devices must be password protected and encrypted
- University-owned devices must have up-to-date security software

8.4 Network Security
- Networks must be secured with firewalls, intrusion detection, and other appropriate measures
- Remote access must be secured with appropriate authentication and encryption
- Regular security scans and updates must be performed

8.5 Physical Security
- Areas where personal data is stored or processed must be physically secured
- Visitor management procedures must be in place

- Clean desk policy must be implemented

8.6 Risk Assessment
- Regular risk assessments shall be conducted
- Security measures shall be adjusted based on risk assessment outcomes

9. DATA SHARING AND TRANSFER

9.1 Internal Data Sharing
- Data sharing between departments shall be documented
- Only the minimum necessary data shall be shared
- Appropriate security measures shall be maintained during internal transfers

9.2 External Data Sharing
When sharing data with external parties:
- Written agreements must be in place
- Due diligence must be conducted on recipients
- Only necessary data shall be shared
- Secure transfer methods must be used

9.3 International Transfers
Transfer of personal data outside Malawi:
- Shall only occur where adequate safeguards are in place
- May require specific consent from data subjects
- Shall comply with relevant international data protection standards
- Shall be documented and approved by the DPO

9.4 Data Processing Agreements
All third parties processing personal data on behalf of the University must enter into a data processing agreement that includes:
- Processing only on documented instructions
- Confidentiality commitments
- Security measures
- Sub-processor restrictions
- Data subject rights assistance
- Breach notification requirements
- Return or deletion of data
- Audit rights

10. DATA RETENTION AND DISPOSAL

10.1 Retention Schedule

- A data retention schedule shall be maintained specifying retention periods for different categories of data
- Retention periods shall be determined based on legal requirements, administrative needs, and good practice
- Different retention periods may apply to different categories of data and individuals

10.2 Review of Retained Data

- Regular reviews shall be conducted to ensure data is not kept longer than necessary
- Data shall be anonymized or pseudonymized where possible if longer retention is required

10.3 Secure Disposal

- Electronic data shall be securely deleted using appropriate methods
- Physical documents shall be shredded or disposed of through secure waste contractors
- IT equipment shall be securely wiped before disposal or reuse

10.4 Documentation of Disposal

Records of destruction shall be maintained for certain categories of sensitive data.

11. BREACH MANAGEMENT

11.1 Breach Detection and Reporting
- All staff must report suspected data breaches immediately to the DPO
- A data breach reporting form shall be available on the University intranet
- 24-hour breach reporting hotline shall be maintained

11.2 Breach Assessment
Upon notification of a suspected breach, the DPO shall:
- Investigate to confirm if a breach has occurred
- Assess the nature and scope of the breach
- Identify affected data subjects and data types
- Evaluate potential consequences and risks

11.3 Breach Response
The University's response to a confirmed breach shall include:
- Containment measures to limit the breach
- Recovery actions to retrieve or secure the data
- Notification to relevant authorities if required
- Communication with affected data subjects if necessary
- Documentation of the breach and response actions

11.4 Breach Register
A register of all data breaches shall be maintained, including:
- Facts about the breach
- Effects of the breach
- Remedial action taken
- Notification details

11.5 Breach Review
Following a significant breach, a review shall be conducted to:
- Identify the root cause
- Evaluate the effectiveness of the response
- Implement measures to prevent recurrence

12. DATA PROTECTION GOVERNANCE

12.1 Data Protection Officer (DPO)

The University shall appoint a Data Protection Officer responsible for:
- Informing and advising on data protection obligations
- Monitoring compliance with data protection regulations
- Providing advice on data protection impact assessments
- Cooperating with supervisory authorities
- Acting as a contact point for data protection issues

12.2 Data Protection Committee

A Data Protection Committee shall:
- Oversee implementation of this policy
- Review data protection practices
- Advise on data protection matters
- Monitor compliance activities

12.3 Departmental Data Protection Coordinators

Each major department shall appoint a Data Protection Coordinator who will:
- Serve as a point of contact for data protection matters
- Assist with implementation of data protection measures
- Report data protection concerns to the DPO

12.4 Responsibility of All Staff

All staff shall:
- Comply with this policy and related procedures
- Report data breaches or concerns promptly
- Complete required data protection training
- Handle personal data in accordance with data protection principles

13. TRAINING AND AWARENESS

13.1 Mandatory Training
- All staff shall receive basic data protection training as part of their induction
- Refresher training shall be provided annually
- Staff handling sensitive data shall receive additional specialized training

13.2 Awareness Activities
- Regular awareness campaigns shall be conducted
- Data protection newsletters shall be circulated
- Data protection resources shall be available on the University intranet

13.3. Training Records
Records of all data protection training shall be maintained.

14. RESEARCH DATA

14.1 Research Ethics and Data Protection
- All research involving personal data must comply with this policy
- Research protocols must be reviewed by the Research Ethics Committee
- Privacy by design principles must be applied to research projects

14.2 Research Participant Rights
- Clear information must be provided to research participants
- Valid consent must be obtained and documented
- Participants must be informed of their rights

14.3 Research Data Management
- Research data management plans must address data protection
- Pseudonymization or anonymization should be used where possible
- Secure storage and transfer methods must be implemented

14.4 Research Data Sharing
- Data sharing agreements must be in place for collaborative research
- Research data may only be shared in accordance with participant consent
- International transfers must comply with section 9.3 of this policy

15. CCTV AND SURVEILLANCE

15.1 Purpose and Scope
- CCTV may be used for security, safety, and crime prevention purposes
- Clear signage must indicate where CCTV is in operation
- CCTV will not be used in areas where there is a reasonable expectation of privacy

15.2 Access to CCTV Footage
- Access to CCTV footage shall be restricted to authorized personnel
- Access requests must be logged
- Footage shall only be viewed in designated secure areas

15.3 Retention of CCTV Footage
- CCTV footage shall normally be retained for 30 days
- Footage related to incidents may be retained longer if necessary for investigation or legal proceedings

15.4 Disclosure of CCTV Footage
- Footage may be disclosed to law enforcement agencies if required by law
- Data subjects may request access to footage of themselves
- Third party images shall be obscured when providing footage to data subjects

16. POLICY IMPLEMENTATION AND COMPLIANCE

16.1 Implementation
- Department heads are responsible for implementing this policy in their areas
- The DPO shall provide guidance on implementation
- Implementation shall be phased according to risk

16.2 Compliance Monitoring
- Regular audits shall be conducted to monitor compliance
- Self-assessment tools shall be provided to departments
- Compliance reports shall be submitted to the Data Protection Committee

16.3 Non-Compliance
- Non-compliance with this policy may result in disciplinary action
- Serious breaches may be treated as gross misconduct
- The University may be liable for fines or penalties for non-compliance with data protection laws

17. REVIEW AND UPDATES

17.1 Policy Review
This policy shall be reviewed:
- Annually
- Following significant changes to data protection legislation
- Following significant data breaches
- As otherwise required

17.2 Policy Updates
- Updates to this policy shall be approved by the University Council
- All staff shall be notified of policy changes
- Updated versions shall be published on the University website and intranet

APPENDICES

Appendix A: Data Subject Request Form
[To be developed]

Appendix B: Data Breach Reporting Form
[To be developed]

Appendix C: Data Protection Impact Assessment Template
[To be developed]

Appendix D: Data Sharing Agreement Template
[To be developed]

Appendix E: Data Retention Schedule
[To be developed]

Appendix F: Privacy Notice Templates
[To be developed]