Kirinyaga University

DOCUMENT: **DATA PROTECTION POLICY**	**REF: KyU/LO/POLICY/001**
CATEGORY: POLICY	**EFECTIVE DATE: 2026** **ISSUE : 1**
PREPARED BY: ……. **LEGAL OFFICER**	**APPROVED BY:** …… **VICE CHANCELLOR**

TABLE OF CONTENTS

FOREWORD

The Bill of Rights under Chapter 4 of the Constitution of Kenya provides that every person has a right to privacy. To further reinforce the right to privacy, the Data Protection Act was enacted in 2019.

In line with the Data Protection Act 2019, the Data Protection Policy is designed to ensure the protection of staff, student, stakeholder and supplier data which is obtained and processed by Kirinyaga University. This Policy is set in place to introduce measures to protect data from data subjects.

The policy addresses the role of the university in use, processing, record keeping, deletion and/or destruction of data.

This Policy applies to all stakeholders, students, teaching and non-teaching staff, suppliers and all other institutions working collaboratively with Kirinyaga University.

Prof. Mary Ndung'u
VICE CHANCELLOR

1. DEFINITION OF TERMS

In this policy, unless the context otherwise requires, the following terms shall have the meanings assigned:

Consent	means any manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject
Data	means "data" means information which is processed by means of equipment operating automatically in response to instructions given for that purpose, is recorded with intention that it should be processed by means of such equipment, is recorded as part of a relevant filing system, or forms part of .in accessible record; or is recorded information which is held by a public entity and does not fall within the above definition
Data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed
Profiling	means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's race, sex, pregnancy, marital status, health status, ethnic social origin, colour, age, disability, religion, conscience, belief, culture, dress, language or birth; personal preferences, interests, behaviour, location or movements
Data Commissioner	means the head of the Office of the Data Protection Commissioner
Data controller	means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of personal data
Data subject	means an identified or identifiable natural person who is the subject of personal data such as an employee, student, supplier or contractor who volunteers their personal data
Data processor	means any supplier that processes personal data on behalf of the data controller, following the controller's instructions

University means Kirinyaga University

2. POLICY OBJECTIVES

The objectives of the Policy are to:

i. Provide guidelines for the collection, storage and erasure of data;
ii. Implement the right to privacy enshrined in the Constitution of Kenya 2010;
iii. To protect personal data collected from various stakeholders;
iv. To set in place procedures that ensure sustainability and transparency in the data lifecycle.

3. SCOPE OF APPLICATION

This Data Protection Policy is applicable to all staff, stakeholders, contractors and students of Kirinyaga University.

4. PURPOSE OF THE POLICY

The Policy seeks to ensure security of data and protect the right to privacy.

5. LEGAL AND POLICY FRAMEWORK

The Data Protection Policy shall be interpreted in accordance with the following;

i. Constitution of Kenya 2010
ii. Data Protection Act 2019 and the guidelines therein
iii. Government Circulars and Regulations
iv. Kirinyaga University Charter of 2016
v. Kirinyaga University Statutes
vi. Universities Act, No. 42, 2012, Laws of Kenya

6. TYPES OF DATA

The University may collect and hold personal data such as:

i. Academic records
ii. Admission records
iii. Attendance and performance data
iv. Background checks
v. Bank account details
vi. Biometric Data
vii. CCTV footage
viii. Consultant records
ix. Contact information
x. Copies of National Identity cards
xi. Copies of passports
xii. Criminal records
xiii. Dates of birth
xiv. Disability or special needs information

xv. Disciplinary records
xvi. Employment contract details
xvii. Financial records such as fees, loans, scholarships
xviii. Gender
xix. Guardians' and sponsors' contact details
xx. Individuals names
xxi. Internet and device usage logs
xxii. Learning management system activity
xxiii. Letters of confirmation
xxiv. Location data
xxv. Medical records including clinician's notes
xxvi. Next of kin names and contacts
xxvii. Passport photos
xxviii. Payroll and tax records
xxix. Photographs and videos
xxx. Referee information for staff or student applications
xxxi. Resumes and qualifications of staff
xxxii. Student Identity cards
xxxiii. Tax PIN, NHIF and NSSF details
xxxiv. University email and system login credentials

7. DATA COLLECTION AND PROCESSING

During data collection and processing, the University shall be guided by the following procedure:

i. The University shall determine the purpose of the data to be collected and ensure that it is legal and necessary to do so.
ii. The University shall determine the data to be collected to achieve the purpose and ensure it is relevant and not excessive.
iii. Where necessary consent shall be obtained from the individuals whose data is being collected. The consent shall be informed, freely given and specific.
iv. Data shall be collected in a lawful and transparent manner, ensuring that it is accurate and up to date; in case of inaccurate data the University shall comply with the data Subject request to edit and update.
v. Data in the University shall be processed in accordance with the purpose for which it was collected and in compliance with relevant data protection laws and regulations (Data Protection Act of 2019 and Data Protection Regulations of 2021).
vi. The University shall ensure that data is stored and protected from unauthorized access, loss, or destruction by putting in place security measures to protect the data such as restricted access, user authentication, data encryption (where applicable).

vii. Review of data collection and processing practices shall be conducted as applicable to ensure compliance with relevant laws and regulations.

8. DUTIES OF THE DATA CONTROLLER AND DATA PROCESSOR

the data controller and processor shall ensure that data is:

i. processed in accordance with the right to privacy of the data subject;
ii. processed lawfully, fairly and in a transparent manner in relation to any data subject;
iii. collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
iv. adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;
v. collected only where a valid explanation is provided whenever information relating to family or private affairs is required;
vi. accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;
vii. kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and
viii. not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.

Further to the above, the data controller shall:

i. obtain valid consent from the data subject where consent is the basis for processing;
ii. facilitate enforcement of data subject rights, such as access, correction, objection to processing and deletion of personal data;
iii. implement technical and organizational measures to protect personal data
iv. conduct data processing impact assessment when data processing is likely to result in high risk to data subjects;
v. notify the Data Commissioner and affected persons of any data breach without undue delay;
vi. ensure that the data processor has a binding agreement in place governing data handling.

9. DATA PROCESSOR

The data processor shall:

i. Process data only on instructions from the data controller;
ii. Have a written binding contract between themselves and the data controller;
iii. Ensure that personnel authorized to process the data are under confidentiality obligations and issue non-disclosure agreements where necessary;

iv. Implement appropriate technical and organizational measures to protect data;
v. Not engage another processor without prior written authorization of the data controller;
vi. Assist the data controller in responding to data subject rights and managing security breaches and impact assessments;
vii. Delete or return data unless otherwise required by law.

10. DATA PROTECTION PRINCIPLES

The following principles for data protection shall apply to Kirinyaga University

i **Lawfulness, fairness and transparency**
Data shall be processed lawfully, fairly and in a transparent manner to the data subject.

ii **Ethics**
The University shall be guided by ethical standards and guidelines when collecting data from individuals. This shall include informed consent, respect for privacy, transparency, responsible use and minimisation of harm.

iii **Purpose limitation**
Data collected and processed must be for a specific and legitimate purpose, and the data should not be further processed in a manner incompatible with that purpose.

iv **Data minimization**
The University shall only collect and process data that is necessary for the purpose of processing.

v **Accuracy**
The data collected shall be accurate and kept up to date.

vi **Storage limitation:**
The data shall be stored for no longer than necessary for the purpose for which it was processed.

vii **Integrity and confidentiality**
University data shall be processed in a manner that ensures its security, confidentiality, and integrity. Appropriate technical and organizational measures shall be put in place to protect the data from unauthorized access, disclosure, alteration, or destruction.

viii **Accountability**
The University shall ensure compliance with applicable data protection laws and regulations.

11. RIGHTS OF A DATA SUBJECT

The data subject has the right to:

i. Consent to the processing and holding of data;
ii. Withdraw consent to processing and holding of data;
iii. Object to the processing and holding of data;

iv. Restrict processing of personal data to a degree acceptable by the data subject;
v. Be informed of the purpose of the collection of data;
vi. Erasure of data;
vii. File a complaint at the office of the data protection commissioner;
viii. Portability of data;
ix. Access data collected by the university;
x. Rectification of data.

Data subjects can enforce their rights by writing to the Vice Chancellor.

12. DATA SHARING AND TRANSFERS

The University may share data with concerned parties such as the government, international institutions, third party contactors, subcontractors and/or their subsidiaries or affiliates who provide support and services to the University for purposes of implementing or effecting or administering and securing any product or service that the data subject is seeking.

The University shall use only third party providers that maintain appropriate levels of security and confidentiality to process personal information only as instructed by the university and to flow the same obligations to their subcontractors and agents.

This clause shall also apply to local and international institutions with which the University has entered into Memoranda of Understanding.

13. DATA RETENTION

The University shall retain data for the period which such data is still in use, and for a period of five (5) years after such use, after which the user department shall conduct the process of erasure/deletion.

During the period of retention, data shall be stored securely and shall not be unreasonably used or disclosed. The University shall apply appropriate security measures such as passwords, encryption, strict access controls and security audits to ensure the secure storage of data.

14. DATA RELEASE AND ACCESS

i. The University shall ensure that access to personal data is limited to authorized persons to fulfill their official duties.
ii. All access to personal data shall be logged, tracked and subject to periodic review.
iii. A data subject may request access to their personal data held by the

University whereupon the University shall confirm whether it holds the requested data, provide access to the data within a reasonable time, and provide information on the purpose of processing, the categories of data processed and any third parties to whom the data has been disclosed.

iv. Any sharing of personal data with external parties shall be governed by a legally binding data sharing or processing agreement;

v. Access requests may be denied in whole or in part where disclosure would:
   (a) Prejudice national security or public interest;
   (b) Reveal confidential information protected by law;
   (c) Infringe on the rights and freedoms of others.

vi. Personal data shall not be released to any third party without the explicit, informed and written consent of the data subject unless:
   (a) The release is required by court order;
   (b) The release is necessary to protect the interests of the data subject;
   (c) The release is in furtherance of a legitimate public interest recognized under law;
   (d) The third party is a contracted data processor and appropriate safeguards and agreements are in place.

15. DATA BREACHES

In the event of a data breach, the data controller shall notify the Office of the Data Protection Commissioner within 3 days of discovery and notify the affected data subjects if the breach is likely to jeopardize their rights and freedoms.

Upon discovery of a data breach, the data controller shall:

i. Contain and assess the extent of the breach;
ii. Document all facts related to the incident;
iii. Take remedial action to mitigate harm and prevent future occurrences;
iv. Maintain a record of all breaches regardless of whether they are notifiable.
v. Subject employees found responsible for data breach to disciplinary action and legal liability if the same occurred as a result of negligence or willful misconduct.

16. DATA SECURITY MEASURES

The University shall apply measures such as passwords, encryption, strict access controls and security audits to ensure secure storage of date.

The University shall conduct periodic trainings for its staff regarding handling of personal data.

17. ROLES AND RESPONSIBILITIES

The University shall appoint Data Protection Officer who will ensure the secure

handling of data by staff, conduct trainings on data protection and handle grievances related to data breaches and breach of rights of data subjects.

18. REVIEW OF POLICY

The Policy will be reviewed every three years or as need arises