DATA PROTECTION POLICY (DPP)

JULY, 2022

APPROVAL DATE BY UNIVERSITY COUNCIL: 9TH SEPTEMBER 2022

APPROVED BY: 

…….

PROF. ISAIAH I.C WAKINDIKI, PhD

VICE-CHANCELLOR& CEO,

CHAIR UNIVERSITY SENATE AND MANAGEMENT BOARD

CONTROL OF DOCUMENT PAGE

Original Issue Date	
Approver	**KCA UNIVERSITY COUNCIL**
Owner	**ICT DEPARTMENT**
Contact Person/ Custodian	**HEAD OF ICT**
Classification	**POLICY**
Approval Date	**KCA UNIVERSITY COUNCIL MEETING HELD ON ……..**
Last Review Date	**JULY, 2022**
Next Review Date	**JUNE, 2025**
Review Frequency	**Every three years**
Version	**1.0**

EXECUTIVE SUMMARY

KCA University Data protection policy is a document with regulations and procedures that shall be adopted to protect and secure all data consumed, managed, and stored by the University. The policy covers all personal data that KCA University holds for either past, current or prospective persons in either electronic or paper format, from when it is created to when it is either destroyed or permanently preserved. It provides the rules of personal data protection, including related obligations of staff, students, research participants, suppliers and other third parties in ensuring responsible processing of personal data.

This policy demonstrates the University's commitment to ensuring adequate level of protection and privacy of personal data as prescribed in the Data Protection Act, No. 24 of 2019.

POLICY PURPOSE

The purpose of this policy is to provide guidelines on how the University shall process the personal data of its staff, students, research participants, suppliers and other third parties in compliance with data protection law and to protect the data subject's rights. The policy shall apply to all personal data the University processes regardless of the format or media on which thedata is stored or to whom it relates

POLICY STATEMENT

KCA University (KCAU) recognises that protecting individuals through legitimate and responsible processing and using their personal data is an imperative human right. The University is committed to complying with the legal requirements contained in the Data Protection Act and other required legislation. All KCAU stakeholders must comply with this policy failure to, which could result in to disciplinary and/or legal actions.

POLICY SCOPE

This policy shall apply to all members of the University, including staff, students, parents, guardians, sponsors, associates, contractors, partners, interns, regulatory bodies and other parties that interact with the University. The scope comprises but is not limited to:- teaching; pedagogic and learning support; research; enterprise and knowledge exchange; human resource administration (including recruitment); student recruitment and admissions; services supporting

the student and academic experience; student registration; progression, and assessment; external engagement and advancement; alumni community management; financial management; facilities management; IT support; legal compliance and corporate governance; and marketing and communications.

DEFINITION OF TERMS

A minor: A person who has not attained the age of majority as per Kenyan law.

Consent: Agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by clear positive action, signifies agreement to the processing of personal data relating to them.

Data Subject: A living, identified or identifiable natural person who is the subject of personal data.

Data Protection Impact Assessment (DPIA): Tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving processing personal data.

Data Protection Officer (DPO): A DPO is responsible for advising the University (including its employees) on their obligations under Data Protection Act, for monitoring compliance with the data protection policy

"DPP" means Data Protection Policy

Health data: Data related to the state of physical or mental health of the data subject

Profiling: Any form of processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular, to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Sensitive personal data: Data revealing the natural person's race, health status, ethnic, social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject.

Third party: A natural or legal person, public authority, agency or other body, other than the data subject, the University or persons who, under the direct authority of the University are authorised to process personal data.

Personal Data: Any information identifying a data subject or information relating to a data subject that can be identified (directly or indirectly) from that data alone or in combination with other identifiers the University possess or can reasonably access. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: Any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data, where that breach results in a risk to the data subject. It can be an act or omission.

Privacy by Design and Default: implementing appropriate technical and organisational measures effectively to ensure compliance with the Data Protection Policy.

Privacy Notices: Separate notices setting out information that may be provided to data subjects when the University collects information about them. These notices may be general privacy statements applicable to a specific group of individuals (for example, employee, student and donor privacy notices or the website privacy policy), or they may be stand-alone, one-time privacy statements covering processes related to a specific purpose.

Processing or Process: Any activity that involves the use of personal data. It includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data, including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties. In brief, it is anything that can be done to personal data from its creation to its destruction, including both creation and destruction.

Pseudonymisation or Pseudonymised: Replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person,to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

LIST OF ACRONYMS AND / OR ABBREVIATIONS

DPA:	Data Protection Act
DPC:	Data Protection Committee
DPIA:	Data Protection Impact Assessment
DPL:	Data Protection Law
DPO:	Data Protection Officer
DPP:	Data Protection Policy
KCAU:	KCA University
PD:	Personal Data

TABLE OF CONTENTS

1.0 INTRODUCTION

KCA University (KCAU) collects and works with certain types of Personal Data about the people with whom it deals, such as current, past and prospective students, employees, and those with whom it communicates. This information is collected for administrative purposes and to fulfil legal obligations to regulatory bodies. The Data Protection Act No 24 of 2019 requiresthat this Personal Data (PD) be processed lawfully, stored safely and not disclosed to any other person or body unless it is necessary to fulfil a contract or meet a legal obligation.

Protecting individuals via the lawful, legitimate and responsible processing and use of their data is a fundamental human right. Individuals may have a varying degree of understanding or concern for protecting their personal data. However, the University must respect their right to have control over their personal data and ensure it acts in full compliance with legislative and regulatory requirements at all times. The Data Protection Policy (DPP) is the main document governing how the University collects and processes personal data. KCAU is committed to protecting the rights and privacy of individuals in accordance with the requirements of the law.

2.0 DATA PROTECTION

2.1 Principles of data protection

KCA University shall ensure that personal data is;

a) Processed in accordance with the right to privacy of the data subject;
b) Processed lawfully, fairly and in a transparent manner in relation to any data subject;
c) Collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
d) Adequate, relevant, limited to what is necessary for relation to the purposes for which it is processed;
e) Collected only where a valid explanation is provided whenever information relating to family or private affairs is required;
f) 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;
g) Kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and

h) Not transferred outside the University unless there is proof of adequate data protection safeguards or consent from the data subject.

2.2 Rights of a Data Subject

A data subject shall have the right to:

a) Be informed of the use to which their personal data is to be put;
b) Access their personal data in the custody of the University
c) Object to the processing of all or part of their personal data;
d) The correction of false or misleading data; and
e) Deletion of false or misleading data about them.

2.3 Exercise of Rights of Data Subjects

A right conferred on a data subject shall be exercised—

a) Where the data subject is a minor, by a person who has parental authority or by a guardian;
b) Where the data subject has a mental or other disability, by a person duly authorised to act as their guardian or administrator; or
c) In any other case, by a person duly authorised by the data subject.

2.4 Collection of Personal Data

a) KCA University shall collect personal data directly from the data subject.
b) KCA University shall collect personal data indirectly where—
    i. The data is contained in a public record;
    ii. The data subject has deliberately made the data public;
    iii. The data subject has consented to the collection from another source;
    iv. The data subject has an incapacity and the guardian appointed has consented to the collection from another source;
    v. The collection from another source would not prejudice the interests of the data subject.
c) KCA University shall collect data from another source if data is necessary for;
    i. The prevention, detection, investigation, prosecution and punishment of crime;

ii. The enforcement of a law which imposes a pecuniary penalty; or
iii. The protection of the interests of the data subject or another person.

d) KCA University shall collect, store or use personal data for a lawful, specific and explicitly defined purpose.

2.5 Duty to notify

KCA University shall, before collecting personal data, in so far as practicable, inform the data subject of—

a) The rights of the data subject as specified under Article 26 of DPA No. 24 of 2019
b) The fact that personal data is being collected;
c) The purpose for which the personal data is being collected;
d) The third parties whose personal data has been or will be transferred to, including details of safeguards adopted;
e) The third-party contacts and whether any other entity may receive the collected personal data;
f) A description of the technical and organisational security measures taken to ensure the integrity and confidentiality of the data;
g) The data being collected pursuant to any law and whether such collection is voluntary or mandatory; and
h) The consequences, if any, where the data subject fails to provide all or any part of the requested data.

2.6 Lawful processing of Personal Data

KCA University shall not process personal data unless;

a) The data subject consents to the processing for one or more specified purposes; or
b) The processing is necessary for;
    i. Performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;
    ii. Compliance with any legal obligation to which the University is subject;
    iii. Protection of the vital interests of the data subject or another data subject;

iv. Performance of a task carried out in the public interest or in the exercise of official authority vested in the University;

v. Performance of any task carried out by a public authority;

vi. The exercise, by any person in the public interest, of any other functions of a public nature;

vii. The legitimate interests pursued by the University by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or

viii. The purpose of historical, statistical, journalistic, literature and art or scientific research.

c) Further processing of personal data shall be in accordance with the purpose of collection.

d) A third party who contravenes the provisions of sub-section (b) commits an offence.

3.0 PROCESSING OF PERSONAL DATA RELATING TO A MINOR

a) KCA University shall not process personal data relating to a minor unless;

i. The minor's parent or guardian gives consent; and

ii. The processing is in such a manner that protects and advances the rights and best interests of the minor.

b) KCA University shall incorporate appropriate mechanisms for age verification and consent to process a minor's personal data.

c) Mechanisms contemplated under sub-section (b) shall be determined based on;

i. Available technology;

ii. The volume of personal data processed;

iii. The proportion of such personal data is likely to be that of a minor;

iv. Possibility of harm to a minor arising out of the processing of personal data; and

v. Such other factors as may be specified by the University.

d) In the event that the University provides services to a minor may not be required to obtain parental consent as set out under sub-section (a) (i).

4.0 RESTRICTIONS ON PROCESSING

a) KCA University shall, at the request of a data subject, restrict the processing of personal data where;
   i. The accuracy of the personal data is contested by the data subject for a period enabling the University to verify the accuracy of the data;
   ii. Personal data is no longer required for the purpose of the processing unless the University requires the personal data for the establishment, exercise or defence of a legal claim;
   iii. Processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; or
   iv. The data subject has objected to the processing, pending verification as to whether the legitimate interests of the University override those of the data subject.

b) Where the processing of personal data is restricted under this section;
   i. The personal data shall, unless the data is being stored, only be processed with the data subject's consent or for the establishment, exercise or defence of a legal claim, the protection of the rights of another person or for reasons of public interest; and
   ii. The University shall inform the data subject before withdrawing the restriction on processing personal data.

c) The University shall implement mechanisms to ensure that time limits are established for the rectification, erasure or restriction of processing of personal data or for a periodic review of the need for the storage of the personal data is observed.

5.0 ACCOUNTABILITY

The University shall:

a) Implement appropriate technical and organisational measures effectively to ensure compliance with data protection principles.
b) Be responsible for and be able to demonstrate compliance with the data protection principles.
c) Apply adequate resources and controls to ensure and document DPP compliance, including:
   i. appointing a suitably qualified DPO;

ii. implementing Privacy by Design when processing personal data and completing a Data Protection Impact Assessment (DPIA) where processing presents a high risk to the privacy of data subjects;
iii. integrating data protection into the University policies and procedures, in the way personal data is handled and by producing required documentation such as Privacy Notices, Records of Processing and records of Personal Data Breaches;
iv. training staff on compliance with Data Protection Law (DPL) and keeping records accordingly; and
v. regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using testing results to demonstrate compliance improvement efforts.

6.0 RESPONSIBILITIES

6.1 University Responsibilities

The KCAU shall establish and implement policies and procedures to comply with data protection laws.

6.2 Data Protection Officer

There is established the office of a Data Protection Officer (DPO) who shall be responsible for:

i. Advising the University and its staff of its obligations under DPP;
ii. Monitoring compliance with this policy and other relevant data protection laws;
iii. Providing advice where requested on data protection impact assessments;
iv. Cooperate with and act as the contact point for the University.

DPO shall, in the performance of his or her tasks, have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of the processing.

6.3 Staff Responsibilities

Staff members who process personal data about students, staff, applicants, alumni or any other individual shall comply with the requirements of this policy.

Staff members shall ensure that:

i. All personal data is kept securely;
ii. No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
iii. Personal data is kept in accordance with the University Records Policy;
iv. Any queries regarding data protection, including subject access requests and complaints, are promptly directed to Data Protection Officer;
v. Any data protection breaches are swiftly brought to the attention of the Data Protection Officer;
vi. Where there is uncertainty around a data protection matter, advice is sought from the Data Protection Officer;
vii. Where staff members are responsible for supervising students doing work which involves processing personal information (for example, in research projects), they shall ensure that those students are aware of the Data Protection principles.
viii. Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data shall seek advice from the Data Protection Officer.

6.4 Third-Party Data Processors

Where external companies are used to process personal data on behalf of the University, the responsibility for the security and appropriate use of that data shall remain with the University.

Where a third-party data processor is used:

i. a data processor shall be appointed to provide sufficient security measures to protect the processing of personal data;
ii. reasonable steps shall be taken to ensure security measures are in place; and
iii. a written and signed contract establishing what personal data shall be processed and for what purpose shall be set out.

The external companies shall be made aware of the DPP and shall guarantee the University that they understand and acknowledge that any disclosure and/or appropriation of any Confidential Information, including by its managers, employees, consultants and/or collaborators, as well as the violation of the legal requirements regarding the protection of the processing of personal data, are of a nature to the cause of serious and irreparable damage to the University. Such violation shall attract such penalties stipulated in the present Contract and the Kenyan Laws on data protection.

6.5 Contractors

All Contractors shall provide the University with the Data in accordance with the terms of this Policy. In so far as Personal data is provided by a Contractor to the University, and/or Processed by the University, both the Contractor and the University qualify as independent Controllers for such Processing.

The terms of engagement between the University and Contractor shall stipulate the responsibilities of the University and that of the Contractor. The Contract shall warrants and give an undertaking that: the Personal data shall be collected, processed and transferred in accordance with the DPP and any other applicable data protection laws.

For purposes of this section, Contractor means a person engaged by the University through a service level agreement or equivalent which provisions require processing of personal data.

6.6 Short-Term and Voluntary Staff

The University shall be responsible for the use of personal data by anyone working on its behalf. short-term or voluntary staff shall be appropriately vetted for the data they shall be processing. University shall ensure that:

i. Any personal data collected or processed in the course of work undertaken for the University is kept securely and confidentially;
ii. All personal data is returned to the University on completion of the work, including any copies that may have been made. Alternatively, the data is securely destroyed, and the University receives notification in this regard from the contractor or short- term/voluntary member of staff;
iii. The University receives the prior notification of any disclosure of personal data to any other organisation or any person who is not a direct employee of the contractor;
iv. Any personal data made available by the University, or collected in the course of the work, is neither stored nor processed outside the University unless written consent to do so has been received from the University;
v. All practical and reasonable steps are taken to ensure that contractors, short-term or voluntary staff do not have access to any personal data beyond what is essential for the work to be carried out properly.

6.7 Student Responsibilities

Students shall be responsible for:

i. Familiarising themselves with this policy when they enrol with the University;
ii. Ensuring that their personal data provided to the University is accurate and up to date.

7.0 OBJECTING TO PROCESSING

A data subject shall have a right to object to processing their personal data unless the University demonstrates compelling legitimate interest for the processing, which overrides the data subject's interests, or for the establishment, exercise or defense of a legal claim.

7.1 Commercial use of data

i. A person shall not use, for commercial purposes, personal data obtained from a data subject pursuant to the provisions of this policy unless the person;
    a) has sought and obtained the express consent from a data subject; or
    b) is authorised to do so under any written law, and the data subject has been informed of such use when collecting the data from the data subject.

ii. Where the University uses personal data for commercial purposes, it shall, where possible, anonymise the data in such a manner as to ensure that the data subject is no longer identifiable.

8.0 RIGHT TO DATA PORTABILITY

i. A data subject shall have the right to receive personal data concerning them in a structured, commonly used and machine-readable format.
ii. A data subject shall have the right to transmit the data obtained under sub-section (i) to a third party without any hindrance.
iii. Where technically possible, the data subject shall have the right to have the personal data transmitted directly from the University to the third party.
iv. The right under this section shall not apply in circumstances where—
    a) processing may be necessary for the performance of a task carried out in the public interest or in the exercise of official authority; or

b) it may adversely affect the rights and freedoms of others.

v. The University shall comply with data portability requests within reasonable timelines; where costs are incurred, the data subject shall bear the cost.

8.1 Retention of Personal Data

i. The University shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed unless the retention is;
   a) Required or authorised by law;
   b) Reasonably necessary for a lawful purpose;
   c) Authorised or consented by the data subject; or
   d) For historical, statistical, journalistic literature and art or research purposes.

ii. The University shall delete, erase, anonymise or pseudonymise personal data not necessary to be retained under subsection (i) in a manner as may be specified at the expiry of the retention period.

iii. This policy shall be read in concurrence with the University Records Policy.

8.2 Right of Rectification and Erasure

i. A data subject may request the University;
   a) To rectify without undue delay personal data in its possession or under its control that is inaccurate, outdated, incomplete or misleading;
   b) to erase or destroy without undue delay personal data that the University is no longer authorised to retain, irrelevant, excessive or obtained unlawfully.

ii. Where the University has shared the personal data with a third party for processing purposes, the University shall take all reasonable steps to inform third parties processing such data that the data subject has requested;
   a) The rectification of such personal data in their possession or under their control that is inaccurate, outdated, incomplete or misleading;
   b) The erasure or destruction of such personal data that the University is no longer authorised to retain, irrelevant, excessive or obtained unlawfully.

iii. Where the University is required to rectify or erase personal data under sub-section (i), but the personal data is required for the purposes of evidence, the University shall, instead of erasing or rectifying, restrict its processing and inform the data subject within a

reasonable time.

8.3 Data Protection by Design or by Default

i. The University shall implement appropriate technical and organisational measures which are designed to;
   a) effectively implement the data protection principles; and
   b) Integrate necessary safeguards for that purpose into the processing.

ii. The duty under subsection (i) applies both at the time of determining the means of processing the data and at the time of the processing.

iii. The University shall implement appropriate technical and organisational measures to ensure that, by default, only personal data which is necessary for each specific purpose is processed, taking into consideration;
   a) the amount of personal data collected;
   b) the extent of its processing;
   c) the period of its storage;
   d) its accessibility; and
   e) the cost of processing data and the technologies and tools used.

iv. The University shall consider measures such as;
   (a) Identify reasonably foreseeable internal and external risks to personal data under the person's possession or control;
   (b) Establish and maintain appropriate safeguards against the identified risks;
   (c) The pseudonymisation and encryption of personal data;
   (d) The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
   (e) Verify that the safeguards are effectively implemented; and
   (f) Ensure that the safeguards are continually updated in response to new risks or deficiencies.

9.0 PARTICULARS OF DETERMINING UNIVERSITY MEASURES

i. In determining the appropriate measures, in particular, where the processing involves the transmission of data over an information and communication network, the University shall have regard to the:
   a) State of technological development available;

b) Cost of implementing any of the security measures;
c) Special risks that exist in the processing of the data; and
d) Nature of the data being processed.

ii. Where the University is using the services of a third party;
a) the University shall opt for a third party who provides sufficient guarantees in respect of university measures;
b) The University shall enter into a written contract which shall provide that the third party shall act only on instructions received from the University and shall be bound by obligations of the University.

iii. The University shall take all reasonable steps to ensure that any person employed by or acting under the authority of the University complies with the relevant security measures.

9.1 Notification and Communication of Breach

i. Where personal data has been accessed or acquired by an unauthorised person, and there is a real risk of harm to the data subject whose personal data has been subjected to the unauthorised access, the University shall;
a) Notify the Data Protection Officer without delay, within forty-eight (48) hours of becoming aware of such breach; and
b) Communicate to the data subject in writing within a reasonably practical period unless the data subject's identity cannot be established.

ii. Where the notification to the Data Protection Officer is not made within forty-eight (48) hours, the notification shall be accompanied by reasons for the delay.

iii. The University may delay or restrict communication referred to under subsection (i)(b) as necessary and proportionate for purposes of prevention, detection or investigation of an offence by the concerned relevant body.

iv. The notification and communication referred to under subsection (i) shall provide sufficient information to allow the data subject to take protective measures against the potential consequences of the data breach, including;
a) Description of the nature of the data breach;
b) Description of the measures that the University intends to take or has taken to address the data breach;

c) Recommendation on the measures to be taken by the data subject to mitigate the adverse effects of the security compromise;

d) Where applicable, the identity of the unauthorised person who may have accessed or acquired the personal data shall be availed to the DPO.

v. The communication of a breach to the data subject shall not be required where the University has implemented appropriate security safeguards, including encryption of affected personal data.

vi. Where and to the extent that it is not possible to provide all the information mentioned in subsection (v) at the same time, the information may be provided in phases without undue delay.

vii. The University shall record the following information in relation to a personal data breach;

a) the facts relating to the breach;

b) its effects; and

c) the remedial action taken.

10.0 PROCESSING OF SENSITIVE PERSONAL DATA

i. No category of sensitive personal data shall be processed unless data protection principles apply to that processing.

ii. Sensitive data shall comprise the following but are not limited to:-natural person's race, health status, ethnicity, social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details, including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject, university records which include minutes, financial records, staff remuneration, templates, establishment, strategic and master plan.

10.1 Personal data relating to health

(1) Personal data relating to the health of a data subject shall only be processed;

(a) by or under the responsibility of a health care provider; or

(b) by a person subject to the obligation of professional secrecy under any law.

(2) The condition under subsection (1) shall be met if the processing;

(a) is necessary for reasons of public interest in the area of public health; or

(b) is carried out by another person who, in the circumstances, owes a duty of confidentiality under any law.

10.2 Protection of Intellectual Property Data

The University recognises the need to protect data generated from ideas, creative activities, innovation and projects from staff and Students. Therefore, this section shall be read in concurrence with the University's Intellectual Property Policy.

10.3 Further categories of sensitive personal data

(1) The University may prescribe further categories of personal data, which may be classified as sensitive personal data.

(2) Where categories of personal data have been specified as sensitive personal data under subsection (1), the University shall specify any further grounds on which such specified categories may be processed, having regard to:

(a) the risk of significant harm that may be caused to a data subject by the processing of such category of personal data;

(b) the expectation of confidentiality attached to such category of personal data;

(c) to whether a significantly discernible class of data subjects may suffer significant harm from the processing of such category of personal data; and

(3)The University shall specify other categories of personal data, which may require additional safeguards or restrictions.

10.4 Automated individual decision making

(1) Every data subject shall have a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning or significantly affects the data subject.

(2) Sub-section (1) shall not apply where the decision is:

(a) Necessary for entering into, or performing, a contract between the data subject and the University;

(b) Authorised by a law to which the University is subject and which lays

down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests; or

(c) Based on the data subject's consent.

(3) Where the University takes a decision which produces legal effects or significantly affects the data subject based solely on automated processing;

(a) the University shall, as soon as reasonably practicable, notify the data subject in writing that a decision has been taken based solely on automated processing; and

(b) After a reasonable period of receipt of the notification, the data subject may request the University to reconsider the decision; or take a new decision that is not based solely on automated processing.

(4) The University, upon receipt of a request under subsection (3), shall within a reasonable period of time ;

(a) Consider the request, including any information provided by the data subject that is relevant to it;

(b) Comply with the request; and

(c) by notice in writing, inform the data subject of— (i) the steps taken to comply with the request; and (ii) the outcome of complying with the request.

(5) The University shall, by this policy, make further provisions to provide suitable measures to safeguard a data subject's rights, freedoms and legitimate interests in connection with making decisions based solely on automated processing.

11.0 GENERAL EXEMPTIONS

(1) Nothing in this Part shall exempt the University from complying with data protection principles relating to lawful processing, minimisation of collection, data quality, and adopting security safeguards to protect personal data.

(2) The processing of personal data shall be exempted from the provisions of this policy if;

(a) it relates to the processing of personal data by an individual in the course of a purely personal or household activity;

(b) if it is necessary for national security or public interest; or

(c) disclosure is required by or under any written law or by order of the court.

11.1 Journalism, Literature and Art

i. The principles of processing personal data shall not apply where—
   a) processing is undertaken by a person for the publication of a literary or artistic material;
   b) the University reasonably believes that publication would be in the public interest; and
   c) the University reasonably believes that, in all the circumstances, compliance with the provision is incompatible with the special purposes.

ii. Subsection (1)(b) shall only apply where it can be demonstrated that the processing is in compliance with any self-regulatory or issued code of ethics in practice and relevant to the publication in question.

11.2 Research, History and Statistics

(1) The further processing of personal data shall be compatible with the purpose of collection if the data is used for historical, statistical or research purposes. The University shall ensure that further processing is carried out solely for such purposes and will not be published in an identifiable form.

(2) The University shall take measures to establish appropriate safeguards against the records being used for any other purposes.

(3) Personal data which is processed only for research purposes is exempt from the provisions of this policy if;
   (a) data is processed in compliance with the relevant conditions; and
   (b) results of the research or resulting statistics are not made available in a form which identifies the data subject or any of them.

(4) The University shall prepare a code of practice containing practical guidance for processing personal data for purposes of Research, History and Statistics.

12.0 DATA PROTECTION COMMITTEE (DPC)

There is established the Data Protection Committee which shall oversee the policy's governance and implementation and provide an oversight role to ensure ethical standards are maintained in the storage, collection, and use of personal data in compliance with the relevant laws.

12.1 Terms of Reference

The terms of reference of the DPC shall be to:

a) Steer the implementation and monitoring of the University's Data Protection policy to foster personal data privacy;
b) Review and make recommendations to the University on the policies, procedures and code of practice in relation to personal data handling and monitoring the implementationof these policies, procedures and code of practice;
c) Develop a personal data inventory for implementation by all units of the University with access to personal data and monitoring the periodic personal data inventory review exercise;
d) Initiate and monitor the periodic risk assessment of all operating units of the University and the privacy impact assessment, when deemed appropriate;
e) Promote staff and students' awareness of data protection and provide training and education to staff members with duties for handling personal data;
f) Formalise and monitor the mechanism for reporting and handling a data breach incident;
g) Review the effectiveness of the University's data protection policy where necessary;
h) Report to the Vice-Chancellor from time to time on matters relating to the University's compliance in relation to data protection.

12.2 Membership Composition

Chair: Deputy Vice-Chancellor Finance, Planning and Development

Secretary: Data Protection Officer

Members: Registrar Academic Affairs

Dean of Students

Head of Human Resources

Head of Finance

Head of ICT

The Committee may invite or co-opt additional Members as resource persons.

13.0 AMENDMENT OF THE POLICY

This policy shall be reviewed after every three (3) years and/or when the need arises.

14.0 REFERENCE

Kenya Constitution of Kenya

Data Protection Act no. 24 of 2019