UNIVERSITY OF NAIROBI

DATA PROTECTION POLICY

2023

TABLE OF CONTENTS

ACRONYMS AND ABBREVIATIONS

AU	-	Africa Union
DPA	-	Data Protection Act
DPIA	-	Data Protection Impact Assessment
DPO	-	Data Protection Officer
ECOWAS	-	Economic Community of West African States
The Act	-	Data Protection Act, 2019
GDPR	-	General Data Protection Regulation
CCPA	-	California Consumer Privacy Act
NCIRT	-	National Computer Incident Response Team
ODPC	-	Office of the Data Protection Commissioner
UoN	-	University of Nairobi
HLCM	-	High Level Committee on Management
UN	-	United Nations

1.0 INTRODUCTION

In Kenya, data privacy is protected by the Data Protection Act, 2019 which provides for the regulation of the processing of personal data. Like other organisations, the University of Nairobi (UoN) must comply with this act's provisions. This includes ensuring that personal data is collected and processed fairly and lawfully, that data subjects are informed of the purpose of data processing, and that appropriate measures are in place to protect the security and confidentiality of personal data.

The University of Nairobi, as a higher education institution, may also collect personal data from students and faculty members for research purposes. In such cases, the university has an ethical responsibility to ensure that data collection and processing practices align with recognized ethical standards and that the privacy rights of research participants are protected.

Overall, it is essential for the University of Nairobi to have strong data privacy policies and procedures in place to ensure compliance with the law and to protect the privacy rights of its data subjects who are students, faculty, and staff. This may include appointing a data protection officer, implementing appropriate technical and organizational measures to protect personal data, and regularly reviewing and updating privacy policies and procedures to ensure they are up to date with legal and regulatory requirements.

1.1 Background

The Kenya Data Protection Act came into force on 25th November 2019 and its aim was to harmonize data privacy in Kenya. Subsequently, several Data Protection Regulations were enacted. Specifically the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 prompted the University to acquire registration as a data controller and data processor in 2023. Consequently, the University is obliged to develop and implement a data protection policy.

This Data Privacy Policy outlines the procedures and guidelines for the collection, use, storage, and protection of personal data by Kenyan University in compliance with the Data Protection Act, 2019. The purpose of this policy is to ensure that the University handles personal data in a lawful, fair, transparent, and secure manner while respecting the privacy rights of individuals.

1.2 Vision, Mission and Philosophy of the University

1.2.1 Vision

A world-class university committed to scholarly excellence

1.2.2 Mission

To provide quality university education and training and to embody the aspirations of the Kenyan people and the global community through creation, preservation, integration, transmission and utilization of knowledge.

1.2.3 Core Values

i. Freedom of thought and expression
ii. Commitment
iii. Trust
iv. Care
v. Excellence
vi. Good governance
vii. Innovativeness and creativity
viii. Partnership and teamwork

1.2.4 Philosophy

The need to connect to and inspire the Kenyan Community, to provide leadership and stewardship and to give hope and faith to the Kenyan society so that it can excel in whatever it chooses to do with passion, moral responsibility and strong sense of patriotism.

1.3 Global, Continental And National Initiatives

1.3.1 Global Initiatives

Data privacy has become an increasingly important issue in the global context due to the widespread use of technology and the internet. With the growth of e-commerce, social media, and the Internet of Things, individuals are generating more personal data than ever before, and there is a growing concern about the security and privacy of this data.

Globally, one hundred and thirty-seven (137) countries out of one hundred and ninety-four (194) countries have put in place legislation to secure the protection of data and privacy. Indeed, UN Global Pulse Principles on Data Protection and Privacy were adopted by the High-Level Committee on Management (HLCM) IN 2018 and the United Nations Sustainable Development Goals Guidance note on big data for achievement of the 2030 Agenda: Data Privacy, Ethics and Protection.

In response to growing concerns about data privacy, several countries and regions have introduced new regulations, such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) in the United States. These regulations aim to give individuals more control over their personal data and to ensure that organizations are transparent about their data collection and use practices.

The COVID-19 pandemic had an impact on data privacy, as governments around the world used contact tracing apps and other data collection measures to track the spread of the virus. While these measures are intended to protect public health, they have also raised concerns about the privacy implications of collecting and using personal data on a large scale.

Overall, data privacy is a complex and evolving issue that requires ongoing attention and vigilance from individuals, organizations, and governments alike.

1.3.2 Continental Initiatives

Numerous countries in Africa have developed or implemented data privacy and security laws in their countries in the last few years. Countries including Ghana, Kenya, Madagascar, Mauritius, Nigeria, Rwanda, South Africa, Togo, Uganda and Zimbabwe have been implementing new measures to protect and secure the personal information of their citizens.

Africa is continuing to strengthen its data protection legal and regulatory framework. Up to February 2023, thirty-six out of fifty-four African countries have data protection laws and/or regulations. Sixteen countries have signed the African Union Convention on Cyber Security and Personal Data Protection adopted on 27 June 2014 (“Malabo Convention") and thirteen countries have satisfied it.

1.3.3 National Initiatives

Kenya has been taking steps to address data privacy concerns in recent years, although there are still challenges that need to be addressed.

In 2019 Kenya passed Kenya's Data Protection Act (DPA) which is the primary legislation governing the collection and processing of personal data. The DPA regulates the processing of personal data, provision of rights of data subjects, creation of the obligations of data controllers, and establishes the Office of the Data Protection Commissioner (ODPC).

In 2020 Kenya enacted the Data Protection (Civil Registration) Regulations, 2020 which regulates the processing of personal data by civil registration entities including registration of births, adoptions, persons, marriages and deaths, and entities responsible for issuing passports and any documents of identity.

In January 2022, a set of three data protection regulations were gazetted and are currently in force:

a) Data Protection (General) Regulations, 2021
b) Data Protection (Registration of Data Controllers, and Data Processors) Regulations, 2021.
c) Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021.

These regulations cater for the procedural aspects of the Kenya Data Protection Act, 2019, and cover a wide spectrum from the transfer of personal data, to how data subjects' rights should be provided for, what the thresholds and requirements are for the registration of data controllers and data processors, how complaints relating to infringements and contraventions of the DPA will be handled and how enforcement procedures will be undertaken.

The government has also established a National Computer Incident Response Team (NCIRT) to respond to and manage cyber threats.

However, there are still concerns about the enforcement of these laws, as well as the lack of awareness and education about data privacy among the general public. There have been reports

of data breaches and unauthorized data sharing by companies and government agencies, highlighting the need for stronger enforcement mechanisms and penalties for non-compliance.

Furthermore, there is a need for greater collaboration and coordination among stakeholders in the Kenyan context. This includes the government, private sector, civil society, and individuals themselves. This collaboration could include developing comprehensive data privacy policies, conducting regular training and awareness-raising activities, and establishing effective reporting and response mechanisms for data breaches.

Overall, while progress has been made in addressing data privacy concerns in Kenya, there is still more work to be done to ensure that individuals' personal data is protected and that the legal framework for data protection is effectively enforced.

1.3.4 The Situation at the University of Nairobi

In general, universities are responsible for collecting, processing, and storing large amounts of personal data related to their students, faculty, and staff, who will henceforth be referred to as 'data subjects'. This data can include sensitive information such as financial records, academic transcripts, and health information.

2.0 GENERAL PROVISIONS

2.1 Definitions

'Anonymisation' means the removal of personal identifiers from personal data so that the data subject is no longer identifiable;

'Biometric data' means personal data resulting from specific technical processing based on physical, physiological or behavioural characteristics including blood typing, fingerprinting, deoxyribonucleic acid analysis, earlobe geometry, retinal scanning and voice recognition;

'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 information which -

a) is processed by means of equipment operating automatically in response to instructions given for that purpose;

b) is recorded with intention that it should be processed by means of such equipment;
c) is recorded as part of a relevant filing system;
d) where it does not fall under paragraphs (a), (b) or (c), forms part of an accessible record; or
e) is recorded information which is held by a public entity and does not fall within any of paragraphs (a) to (d).

'Data Commissioner' means the person appointed as prescribed in the Data Protection Act, 2019.

'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 Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller;

'Data Subject' means an identified or identifiable natural person who is the subject of personal data;

'Encryption' means the process of converting the content to any readable data using technical means into coded form;

'Filing System' means any structured set of personal data which is readily accessible by reference to a data subject or according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

'Health Data' means data related to the state of physical or mental health of the data subject and includes records regarding the past, present or future state of the health, data collected in the course of registration for, or provision of health services, or data which associates the data subject to the provision of specific health services;

'Identifiable Natural Person' means a person who can be identified directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or social identity;

'National Security Organs' has the meaning assigned to it under Article 239 of the Constitution;

'Office' means the office of the Data Protection Commissioner

'Person' has the meaning assigned to it under Article 260 of the Constitution;

'Personal data' means any information relating to an identified or identifiable natural person;

'Personal 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;

'Processing' means any operation or sets of operations which is performed on personal data or on sets of personal data whether or not by automated means, such as

a) collection, recording, organization, structuring;
b) storage, adaptation or alteration;
c) retrieval, consultation or use;
d) disclosure by transmission, dissemination, or otherwise making available; or
e) alignment or combination, restriction, erasure or destruction.

'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 analyze 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.

'Pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject with the use of additional information, and such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

'Restriction of Processing' means the marking of stored personal data with the aim of limiting their processing in the future;

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

'Third party' means a natural or legal person, public authority, agency or other body, other than the data subject, data controller, data processor or persons who, under the direct authority of the data controller or data processor, are authorized to process personal data.

2.2 Legal and Policy Framework on Data Privacy

The University policy will abide by the applicable legal instruments and institutional policies for data privacy as outlined below:

2.2.1 International Instruments:

a) Treaties and Conventions ratified by Kenya.

2.2.3 Legislative Framework

a) Constitution of Kenya, 2010
b) The Employment Act, 2007
c) The Data Protection Act, 2019

2.2.4 Policies and Guidelines Framework

a) University of Nairobi Policies and Guidelines.

3.0 POLICY STATEMENT

In keeping with its vision, mission, and core values, the UoN aspires to be a world-class university, which is committed to academic excellence and transformation of the lives of Kenyans while serving the society with distinction.

The University of Nairobi is committed to protecting the privacy of the personal data it collects and processes. The University recognizes the importance of data privacy and understands that customers, employees, and partners trust the University to handle their personal data responsibly.

The University collects personal data only for specific purposes and with appropriate legal basis, such as performance of contract, consent or legitimate interests. The University takes appropriate technical and organizational measures to protect personal data against unauthorized access, accidental loss, or damage, and to regularly review and improve on the security measures to ensure the ongoing protection of personal data.

The University provides clear and transparent information to individuals about the types of personal data collected, how it is used, and with whom it is shared. The University respects individual privacy rights such as the right to access, rectify, erase, restrict, or object to the processing of personal data.

The University complies with all applicable data protection laws and regulations, including the Data Protection Act, 2019 and other applicable laws. The University will regularly review and update the data privacy policies and procedures to ensure that they are in line with legal and regulatory requirements and industry best practices.

The University of Nairobi takes data privacy responsibilities seriously, and it is committed to maintaining the trust of our students, staff and partners by protecting their personal data with the highest standards of security and privacy.

4.0 RATIONALE AND JUSTIFICATION

4.1 Rationale for the Data Protection/Privacy Policy

There are several reasons why the University of Nairobi should have a strong data privacy policy in place. These reasons include;

a) Protection of personal information: Data privacy policies help to ensure that personal information collected by the university is processed and handled in a manner that respects the privacy rights of individuals. This includes ensuring that personal data is collected and processed only for specific purposes and that data subjects are aware of their rights with respect to their personal data.
b) Ethical considerations: Data privacy policies are not just a legal requirement but also an ethical responsibility. The university has an obligation to protect the privacy and security of personal data and to ensure that data subjects are aware of their rights with respect to their personal data.
c) Reducing risks: Organizations that have weak data privacy policies are at risk of data breaches, which can be costly in terms of financial losses and damage to reputation. By implementing strong data privacy policies and procedures, organizations can reduce the risks of data breaches and ensure that personal data is handled securely.
d) Legal compliance: As mentioned earlier, data privacy is regulated by various laws and regulations, such as the Data Protection Act, of 2019. The University is required to comply with these laws, failure to which may result in data breaches, penalties, fines, or legal action.
e) Maintaining trust: Organizations that have strong data privacy policies in place are more likely to maintain the trust of their customers, clients, and other stakeholders. By demonstrating a commitment to protecting personal data, organizations can build and maintain strong relationships with their stakeholders, which can be beneficial in terms of reputation and brand loyalty.

In summary, having strong data privacy policies is essential for the University of Nairobi to comply with legal and regulatory requirements, protect personal information, maintain trust with stakeholders, reduce risks, and uphold ethical standards.

4.2 Justification for a Data Privacy Policy

A data privacy policy is essential for the University of Nairobi to protect the privacy of individuals, comply with legal and regulatory requirements, build trust with stakeholders, and mitigate risks associated with handling personal data.

5.0 THE PURPOSE, GOAL AND OBJECTIVES

5.1 Policy Purpose

The purpose of a data privacy policy is to establish guidelines and procedures for the collection, use, storage, sharing, and protection of personal data.

A data privacy policy is important because it helps to ensure that the university complies with legal and regulatory requirements related to data privacy. It also helps to build trust with students, staff, parents and guardians, and other stakeholders by demonstrating a commitment to protecting their privacy rights.

A well-crafted data privacy policy can help to mitigate the risk of data breaches, identity theft, and other forms of cybercrime. It can also help to avoid reputational damage and financial penalties that can result from non-compliance with data privacy regulations.

In addition, a data privacy policy can help the university to manage the risks associated with data collection and processing, and to establish best practices for data handling that promote transparency, accountability, and ethical behavior.

Overall, a data privacy policy is an essential tool for the university as it collects and processes personal data, and it helps to protect the privacy rights of individuals and to promote a culture of responsible data management.

5.2 Policy Goal

The goal of this data privacy policy is to protect the privacy and confidentiality of personal data that the University of Nairobi collects, processes, and stores. This policy outlines the university's

approach to data privacy, including the types of data collected, the purposes for which the data is used, and the measures in place to protect the data from unauthorized access or disclosure.

The primary goal of this policy is to ensure that individuals have control over their personal data and are aware of how their data is collected, processed, and used in order to create trust and awareness of how their personal data is protected throughout the data lifecycle.

5.3 Policy Objectives

The main objectives of this policy are to;

a) Define the personal data that is collected from the data subjects, ensure that only necessary data is collected and that individuals are informed of the purposes of data processing.
b) Establish guidelines for obtaining consent from students and staff for the collection, processing, and sharing of their personal data.
c) Set standards for the security and confidentiality of personal data, including measures for protecting data against unauthorized access, use, and disclosure.
d) Provide procedures for handling data breaches, including reporting and notification requirements.
e) Define the rights of individuals with respect to their personal data, including the right to access, rectify, and delete their data.
f) Establish processes for monitoring and enforcing compliance with the policy, including regular audits and training for staff.
g) Ensure that the policy is reviewed and updated regularly to ensure ongoing compliance with changing prevailing laws and regulations.

6.0 PRINCIPLES OF DATA PROTECTION

The principles enumerated below are aimed at the following three outputs: harmonize standards for the protection of personal data; facilitate accountable processing of personal data and ensure respect for human rights and fundamental freedoms of individuals, in particular the right to privacy.

The University shall, in accordance with Section 25 of the Data Protection Act, 2019 ensure that 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** in 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 Kenya**, unless there is proof of adequate data protection safeguards or consent from the data subject.

i) protected by putting in place organizational and technical measures that guarantee the security of personal data

j) handled in a manner that upholds the integrity and confidentiality of the data by authorized personnel

k) processed, stored and used with sufficient technical safeguards as prescribed in Section 41 of the DPA

l) pseudonymised or anonymised during processing that includes Collaboration and data transfer in accordance with applicable laws.

m) stored and retained in accordance with the University policy on Records Management.

7.0 SCOPE AND APPLICATION

This policy applies to all personal data, controlled and processed by the University of Nairobi including data held in electronic and paper format. Including but not limited to the following:

7.1 Types of Data

7.1.1 Student Data

7.1.2 Research

7.1.3 Human Resource

7.1.4 Financial Data

7.1.5 Sensitive Data

8.0 PROCESSING AND USE OF PERSONAL DATA

8.1 Collection

The University will obtain consent from data subjects prior to collecting their personal data unless the processing is necessary for teaching and learning as per the provisions of the Data Protection Act, 2019. Consent obtained from the data subject should demonstrate manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or clear affirmative action signifying agreement to the processing of personal data related to the data subject.

8.2 Storage

The University shall store personal data with both organizational and technical measures put in place to guarantee the security and privacy of personal data.

8.3 Retention

The University shall limit the collection, processing and retention of personal data to the specific purpose of achieving its mandate as prescribed in the Universities Act and the University of Nairobi Charter,2013 and the Retention and Disposal Policy and Schedules of Records, 2019.

8.4 Personal Data Relating to Health

The University shall collect and process personal data relating to the health of a data subject in order to foster general wellbeing of staff and students.

Personal Data relating to health shall be collected and processed under the responsibility of a health care provider or by a person subject to the obligation of professional secrecy under any law.

Processing of personal data related to health shall be deemed necessary for reasons of public interest in the area of public health.

.

8.5 Third-Party Sharing

The University shall not share personal data with third parties unless the data subject has given explicit consent, or in instances where such sharing is obligated under the Constitution of Kenya, 2010, The Act or any other enabling provisions of applicable Laws, or if the sharing is necessary for the specific purpose for which the data was collected and with appropriate safeguards in place.

Third parties that the university is mandated to share data with by law will not require a contractual agreement prior to sharing of data; however, those without this mandate shall be contractually bound to comply with the law and our policies and regulations.

Third parties from other jurisdictions shall in addition to compliance with the relevant Laws applicable in Kenya be required to demonstrate conformity with data protection principles applicable in their respective jurisdictions.

The university shall be guided by the law and contractual agreements when receiving or giving data to and from third parties.

8.6 Transfer of Personal Data Outside The Country

The University will not transfer or process personal data outside the country unless there is proof of adequate data protection safeguards or consent from the data subject. Further to this, the

University shall not transfer or process personal data that is highlighted in section 25 of the Data Protection General Regulations, 2021 outside the country.

8.7 Records Archival

The University shall archive records, in accordance with the Data Protection Act, 2019, for historical, research and informational purposes as well as for institutional memory. This shall also be guided by the University Policy on Records Management.

8.8 Removal and Storage Limitations

Removal of personally identifiable information and storage limitations are governed by Section 39 of the DPA and the Records Retention Policy of the university.

8.9 Access to Data

The university will uphold the right of the data subject to access their personal data and guarantee protection against unauthorized access in line with the university policies.

8.10 Correction of Personal Data

The University will ensure that personal data collected by the University is captured correctly as availed by the data subject or third-party providers. The University will provide data subjects with the right to have their data corrected or rectified within a reasonable period upon receipt of an appropriate official communication from the data subject or a third party of an error.

9.0 RESPONSIBILITIES

9.1 Data Controller

The University shall determine what personal data shall be collected, the purpose for which it shall be processed and implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing of personal data is performed in accordance with the Act and internal policies. The University will take into account the nature, scope, context and purposes of the processing.

9.2 Data Processor

The University shall carry out processing activities according to the duration, nature and purpose of the processing, the type of personal data and categories of data subjects while protecting the rights of a data subject and in accordance with the Act.

9.3 Data Protection Officer

In compliance with the Act Section (24) the University shall appoint a Data protection officer who will be responsible for overseeing compliance with the Data Protection Act and this policy.

The duties and responsibilities of the data protection officer are:

a) Advise the University of Nairobi on data processing requirements provided under The Act or any other written law;
b) Ensure on behalf of the University that this Act is complied with;
c) Facilitate capacity building of staff and students involved in data processing Operations;
d) Provide advice on data protection impact assessment; and
e) Cooperate with the Data Commissioner and any other authority on matters relating to data protection.
f) Receive and resolve complaints on data privacy breaches from data subjects.

9.4 Records Manager

The records manager has the responsibility to carry out the following operations and responsibilities of records management in a manner that protects personal data and adheres to the DPA, 2019.

a) Records use and maintenance
b) Records disposal
c) Records archival
d) Mail management
e) File and document management

9.5 Data Subjects (Students and Staff)

9.5.1 Students

a) Whereas the University shall provide the technical and organizational security measures that will ensure integrity and confidentiality of data, students are also responsible for not exposing and maintaining the confidentiality and security of their personal data, as well as any sensitive information they may provide as part of their academic activities.
b) Prior to providing consent for the collection, use, and disclosure of their personal data, it is expected that a student shall have understood the purpose for the collection, use and/or disclosure of such data by the university and its authorized personnel.
c) Students should be aware of the university's data protection policies and guidelines, including any specific requirements for handling personal information, such as research data or participant information.
d) Students should promptly report any breaches or incidents involving the unauthorized access, loss, or disclosure of personal data to the relevant university authorities.
e) Students should adhere to the university's data protection policies and guidelines, following any specific instructions or protocols for handling, storing, or transmitting personal data.

9.5.2 Staff

a) Staff tasked with the responsibility of handling or processing data subjects' personal data shall be responsible for the confidentiality, security, integrity and ethical use of the data.
b) Staff tasked with the responsibility of collecting and processing data subjects' personal data should only collect and process data that is necessary for legitimate purposes, and not retain it longer than required or beyond the consent provided or the relevant legal policy provision.
c) Staff members must comply with the security measures (see clause 8.2 and clause 8.8) put in place by the University to protect personal data in their custody from unauthorized access, loss, or alteration.
d) Staff should receive regular training on data protection and privacy practices to stay updated with the latest guidelines and best practices.
e) Staff members should comply with relevant data protection laws and regulations, as well as the university's internal policies and procedures regarding the handling of personal data.

f) Staff should promptly report any data breaches, security incidents, or unauthorized access to personal data to the designated university authorities.
g) Staff members should provide guidance and support to students in collaboration with the Data Protection Officer regarding data protection practices, ensuring that students are aware of their rights and responsibilities.
h) Staff are responsible for not exposing and maintaining the confidentiality and security of their personal data, as well as any sensitive information they may provide as part of their duties.
i) Prior to providing consent for the collection, use, and disclosure of their personal data, it is expected that staff shall have understood the purpose for the collection, use and/or disclosure of such data by the university.
j) Staff should be aware of the university's data protection policies and guidelines, including any specific requirements for handling personal information, such as research data or participant information.

9.6 Responsibility of Management

The University Management and the heads of units shall determine the purposes and means of processing personal data. Management shall also ensure that the rights and freedoms of data subjects are protected as prescribed in the Data Protection Act, 2019 and in all the internal policies and guidelines within their allocated responsibilities by the Data Controller.

10.0 RIGHTS OF DATA SUBJECT

A data subject of the University shall have a right to -

a) be informed of the use to which their personal data is to be put;
b) access their personal data held by the University;
c) request correction of their personal data if it is inaccurate, incomplete, or out of date;
d) object to the processing of their personal data for certain purposes
e) request deletion of false or misleading data about them.

11.0 DATA MINIMIZATION

The University shall practice data minimization by:

a) Collecting and processing personal data that is necessary to achieve specific purposes.
b) Ensure that the collected personal data is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
c) Taking all reasonable steps to ensure that personal data that is no longer necessary is deleted or anonymized.
d) Ensuring that personal data is not disclosed to any third party unless necessary for the specific purpose and with appropriate safeguards in place.

12.0 DATA SECURITY

a) The University will implement appropriate technical and organizational measures to ensure the security of personal data.
b) Access to personal data will be restricted to authorized personnel who have a legitimate need to access the data.
c) Personal data will be protected by appropriate physical, technical, and administrative measures to prevent unauthorized access, disclosure, or destruction.
d) The University will regularly review and update its security measures to ensure that they remain effective.

13.0 DATA PROTECTION MEASURES

Any processing of personal data deemed risky shall be required to undergo a Data Protection Impact Assessment (DPIA) prior to the processing as outlined in section 31 of the Act and submitted to Management for further action.

The University will ensure that appropriate security measures are in place to protect personal data from unauthorized access, disclosure, or destruction.

14.0 DATA PROTECTION INCIDENTS AND BREACHES

a) All data breaches or incidents shall be reported to the Data Protection Officer.

b) The University will notify data subjects and the relevant authorities of any data breaches that may pose a risk to their rights and freedoms.

c) The University will promptly investigate any suspected or actual data breaches and take appropriate action to mitigate any harm.

15.0 MONITORING AND EVALUATION OF ENFORCEMENT

Section 31 of the DPA requires that where processing will result in a high risk to the rights of a data subject a DPIA shall be carried out.

Further to the roles and responsibilities of the Data Protection Officer and the University Management, (See Section 9.0) the responsibility of monitoring and evaluation of compliance shall also be on all staff, students, researchers and third-party stakeholders who interact with personnel data in the process performing their duties or in the process of undertaking the obligations and mandate of the University.

15.1 Compliance Assessment

The Data Protection Officer shall, from time to time, hold Data Protection Impact Assessments (DPIA) as part of following up and checking on compliance.

The DPIA form (ANNEX I) shall be used to assess compliance. Any instances of potential risks of breach shall be reported and measures taken as appropriate. In this respect, the heads of the various units (Heads of Departments/Divisions, Deans/Directors, and DVCs), guided by the DPO will carry out DPIAs for self-assessment.

16.0 POLICY REVIEW

This policy will be reviewed and updated periodically to ensure that it remains current and compliant with the DPA.

17.0 DOCUMENT CHANGES

Date	Clause	Authorized By
February 2nd, 2024	Approval of Draft Data Policy	UEB
	Approval of Draft Data Policy	Council

ANNEX I: DATA PROTECTION IMPACT ASSESSMENT TEMPLATE

Instructions

1. Fill out this template prior to the commencement of any processing activity of personal data, or if you are making a significant change to the existing process.
2. Integrate the final outcomes back into your project plan.

Part 1: Description of the processing operations

1. Project Name	
2. Project Outline: What and why. *(Explain broadly what the project aims to achieve and what type of processing it involves)*	
3. Who are the targeted data subjects? a. What are the classes of data to be collected; b. What is the class of data subjects (i.e. are there any vulnerable groups/children that form part of the data subjects)	
4. Describe the information flow. *Describe the collection, use and deletion of personal data here. It may be in a flow diagram or another format of explaining data flows*	
a) Where you are getting the data from; *b) how is the data being collected;* *c) how much data is likely to be collected;* *d) where the data will be stored;* *e) how long will the data be stored;* *f) To what extent is the data being processed* *g) where data could be transferred to; and,* *h) how many individuals are likely to be affected by the project.*	

5. Describe how the data processing flow complies with the data protection principles a) Lawfulness, fairness and transparency b) Purpose limitation c) Data minimisation d) Accuracy e) Storage limitation f) Integrity and confidentiality g) Accountability	

Part 2: An assessment of the necessity and proportionality of the processing operations in relation to the purpose.

Describe compliance and proportionality, measures, in particular:	
1. What is your lawful basis for processing?	
2. How is the consent to be obtained, if at all?	
3. Does the processing actually achieve your purpose?	
4. Is there another way to achieve the same outcome?	
5. How will you ensure data quality and data minimization?	
6. What information will you give individuals?	
7. How will you help to support their rights?	
8. What measures do you take to ensure compliance by the Controller and Processor?	
9. What parties are involved in the processing and what are their specific roles?	
10. How do you safeguard the processing of personal data?	
11.How do you safeguard any international transfers?	

Part 3: An assessment of the risks to the rights and freedoms of data subjects.

ASSESSMENT QUESTIONS

Explain what practical steps you will take to ensure that you identify and address privacy risks.	**Yes. (Please give an explanation)**	**No. (Please give an explanation)**
1. Will the project involve the collection of new identifiable or potentially identifiable data about data subjects?		
2. Will the project compel data subjects to provide information about themselves, i.e., where they will have little awareness or choice?		
3. Will identifiable information about the data subjects be shared with other organizations or people who have not previously had routine access to the information?		
4. Are you using information about data subjects for a purpose it is not currently used for in a new way, i.e. using data collected to provide for an evaluation of service development.		
5. Where information about data subjects is being used, would this be likely to raise privacy concerns or expectations, i.e. will it include health records, criminal records or other information that people may consider to be sensitive and private and may cause them concern or distress?		
6. Will the project require you to contact data subjects in ways that they may find intrusive, such as telephoning or emailing them without their prior consent?		

7. Will the project result in you making decisions in ways which can have a significant impact on data subjects, i.e. will it affect the services a person receives?		
8. Does the project involve you using new technology which might be perceived as being privacy intrusive, i.e. using biometrics, facial recognition or automated decision-making?		
9. Is a service being transferred to a new supplier (re-contracted) and the end of an existing contract?		
10. Is processing of identifiable/potentially identifiable data being moved to a new organization (but with the same staff and processes)		

Part 4: The measures envisaged for addressing the risks and the safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Data Protection Act.

Risk Assessment - Identifying Privacy Risks and Evaluating Privacy Solutions								
Risk ID	**Risk Description**	**Consequence**	**Risk Owner**	**Current internal CONTROLS (provide details of how you currently manage the risk)**	**Assessment of Risk**			**Describe what further ACTIONS you will take to <u>reduce the Impact/Likelihood</u> and mitigate the risk. State who is the risk owner for each action**
					Impact (1,2,3,4,5)	*Likelihood (1,2,3,4,5)*	*Score*	

Part 5: Sign Off and Record Outcomes

ITEM DESCRIPTION	OFFICER NAME/DATE	NOTES/INSTRUCTIONS
Measures approved by:		Integrate actions back into the project plan, with the date and responsibility for completion.
Residual risks approved by::		If accepting any residual high risk, consult the ODPP before going ahead
DPO advice provided:		DPO should advise on compliance, PART 4 measures and whether processing can proceed.
Summary of DPO advice:		
DPO advice accepted or overruled by::		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		
Comments		
Consultation with Office of the Data Protection Commissioner.		
Response		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA.

Dated: ……..

Signed by: …….

Department: ……

UNIVERSITY OF NAIROBI

University of Nairobi Students Privacy Notice

The University of Nairobi provides access to services and information online in a manner that respects and protects your privacy. This statement describes the information-collection practices and explains how it uses and protects your personal information.

This Privacy Policy describes the University's practices in connection with information that it collects through;

- websites operated by the University from which you are accessing this Privacy Policy (the "**Websites**")
- the management information systems made available and accessible by the University through electronic systems, computers and mobile devices (the "**Systems**"),
- University social media sites
- emails and electronic messages
- offline activities as defined in the University policies, procedures and guidelines
- "**Services**" refers to the Websites, MIS Systems and Social Media sites.

Personal Data

"**Personal data**" identifies you as an individual or relates to information relating to an identifiable natural person, **including, but not limited to**:

- Name
- Postal address
- Telephone number
- Email address
- National ID Number
- Signatures
- Biological identifiers
- Personal data images
- Biometric details
- Through information you voluntarily provide through use of University Services, and may include sensitive information, such as health, financial, racial and ethnic origin information.

Collection of Personal Data

The university collects Personal data in a variety of ways, including:

- **Through University Services** when you access or use University Services, register to access Services, make payments, biometric registration or through engaging in any other University activities that invoke the policies, procedures and guidelines.
- **The University** collects personal data from you offline, e.g., when you visit our campuses or other facilities, attend one of our seminars, place a request over the phone, or contact the University.
- **Other Sources**
    - The University may receive your personal data from other sources, for example publicly available databases or interacting with University social media sites.

- Other partners when they share the information with the University;

    - *If you disclose any personal data relating to other people to the University or to our third-party service providers in connection with the Services, you represent that you have the authority to do so,* and that you undertake to indemnify and keep us indemnified against all liability arising out of the disclosure or use of such information including all actions, suits, proceedings, claims, costs and expenses that may be taken against us as a consequence of such information having been in our possession and use.

Use of Personal Data

The University will use or share with third parties personal data as prescribed in the Act for legitimate business purposes including:

- Providing the functionality of the Services and fulfilling your requests. To provide the Services' functionality to you, such as providing access to your student portal account as well as a University email account, and providing you with related services or communications. If you do not provide the information requested, we may not be able to provide the Services' functionality.
- Responding to your inquiries and fulfilling your requests, when you contact us via one of our online contact forms or otherwise, for example, when you send us questions, suggestions, compliments or complaints, or when you request other information.
- Completing your transactions, to provide you with related services or communications.
- Sending administrative information to you, such as changes to our offerings, terms, conditions and policies.
- Allowing you to send messages to another person if you choose to do so. The University will engage in these activities to manage our relationship with you and/or to comply with any legal obligation.
- Providing you with our newsletters and/or other promotional materials and facilitating social sharing
- Sending you promotional-related emails, with information about University services, offerings, new initiatives and other news about the University.
- Facilitating social sharing functionality that you choose to use.

The University will engage in the under-noted activities with your consent or where we have a legitimate interest.

- **Analysis of Personal Information for reporting and providing personalized services.**
    - To analyze or predict its users' preferences in order to prepare aggregated trend reports on how our digital content is used, so it can improve University Services.
    - To better understand you, so that the University can personalize our interactions with you and provide you with information and/or offers tailored to your interests.
    - To better understand your preferences so that the University can deliver content via University Services that it believes will be relevant and interesting to you.
- **Aggregating and/or anonymizing Personal Data.**
    - The University may aggregate and/or anonymize personal data so that it will no longer be considered personal data. It does so to generate other data for its use, which it may use and disclose for any purpose.
- **Subject to your consent or in instances where it is permitted by written law, the University may use your personal data for its business and operational purposes as stated below;**
    - For data analysis, for example, to improve the efficiency of University Services;
    - For audits, to verify that University internal processes function as intended and are compliant with legal, regulatory or contractual requirements;
    - For fraud and security monitoring purposes, for example, to detect and prevent cyber attacks or attempts to commit identity theft;
    - For developing new offerings, initiatives and services;
    - For enhancing, improving, or modifying University current offerings, initiatives and services;
    - For identifying usage trends, for example, understanding which parts of University Services are of most interest to users;
    - For determining the effectiveness of University promotional and informational campaigns, so that we can adapt our campaigns to the needs and interests of University users.

Disclosure of Personal Information

The University may disclose Personal Information **to third parties to facilitate the services they provide to the University, which are necessary for the performance of the contract between the University and the students;**

- These can include providers of services such as data analysis, payment processing, event registration, information technology and related infrastructure provision, customer service, email delivery, auditing, and other services.

- **By using the University Services, you may elect to disclose personal data**
    - On message boards, chat, profile pages, blogs and other sites to which you are able to post information and content (including, without limitation, University Social Media Sites).

    - Through your social sharing activity. When you connect your Services account with your social media account, you will share information with your friends associated with your social media account, with other users, and with your social

media account provider. By doing so, you authorize the University to facilitate this sharing of information, and you understand that the use of shared information will be governed by the social media provider's privacy policy.

Please note that any information you post or disclose through these services will become public and may be available to other users and the general public.

Other Uses and Disclosures

The University may use and disclose your personal data when it has a legal obligation or legitimate interest to do so. This may include:-

- **To comply with applicable law and regulations within its jurisdiction or comply with a contractual obligation to which the students are parties.** Disclosure of data outside the country is subject to Section 25 (f) of the Data Protection Act. Either consent from the data subject should be availed or there should be proof of adequate data protection safeguards.
- **To cooperate with the government and its agencies**
- **To cooperate with any other law enforcement agency within its jurisdiction**
- **For compliance with any legal obligation to which the University is a party**

Other Information

"**Other Information**" is any information that does not reveal your specific identity or does not directly relate to an identifiable individual

- Browser and device information
- System usage data
- Information collected through cookies and other technologies
- Demographic information and other information provided by you that does not reveal your specific identity
- Information that has been aggregated in a manner such that it no longer reveals your specific identity

If the University is required to treat Other Information as Personal Information under applicable law, then it may use and disclose the information for the purposes for which it uses and discloses Personal Information as detailed in this Policy.

Collection of Other Information

The University may collect other information in a variety of ways, including;

- **Through your browser or device:**
  - Certain information is collected by most browsers or automatically through your device. The University may use this information to ensure that the Services function properly.

- **Through your use of the Systems**
  - When you use the Systems, The University may track and collect system usage data.

- **Using cookies**
  - Cookies are pieces of information stored directly on the computer that you are using. Cookies allow the collection of information such as browser type, time spent on the Services, pages visited, language preferences, and other traffic data. The University may use the information for security purposes, to facilitate navigation, to display information more effectively, and to personalize your experience.

- **Using technology to track the use of services and improve the services**
- **Analytics**. In some instances, the University may use Google Analytics, which uses cookies and similar technologies to collect and analyze information about the use of the Services and report on activities and trends. This service may also collect information regarding the use of other websites, apps and online resources.
- **IP Address**
    - Your IP address is automatically assigned to your computer by your Internet Service Provider. An IP address may be identified and logged automatically in our server log files whenever a user accesses the Services, along with the time of the visit and the page(s) that were visited. Collecting IP addresses is standard practice and is done automatically by many websites, applications and other services. IP addresses are used for purposes such as calculating usage levels, diagnosing server problems and administering Services. Your approximate location may also be derived from your IP address.

Uses and Disclosures of Other Information

The University may use and disclose Other Information for specific purposes, (Pursuant to Data Protection Act,2019) except where it is required to do otherwise under applicable law.

Security

The University seeks to use reasonable organizational, technical and administrative measures to protect personal data within the University. Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with the University is no longer secure, please immediately notify it in accordance with the *"Contacting Us"* section below.

Choices and Access

Your choices regarding the University's use and disclosure of your personal data. The University will seek your consent regarding our use and disclosure of your personal data for promotional purposes in accordance with our Data Privacy policy. You may opt-out of receiving electronic communications from us. If you no longer want to receive promotional-related emails from the University on a going-forward basis, you may opt-out according to instructions in such communications.

The University will try to comply with your request(s) as soon as reasonably practicable. Please note that if you opt out of receiving marketing-related emails from the University, we may still send you important administrative messages, from which you cannot opt out.

Access to change or deletion of your Personal Data

To the extent these rights are provided to you by applicable law, if you would like to request to review, correct, update, suppress, restrict or delete personal data that you have previously provided to the University, object to the processing of personal data or if you would like to request to receive an electronic copy of your personal data for purposes of transmitting it to another entity, please contact the University at **vc@uonbi.ac.ke** We will respond to your request consistent with applicable law.

Retention Period

The University will retain Personal Information for as long as needed or permitted in light of the purpose(s) for which it was obtained and consistent with applicable law.

The criteria used to determine our retention periods include:

- The length of time we have an ongoing relationship with you and provide the Services to you (for example, for as long as you have an account with the University or keep using the Services);
- Whether there is a legal obligation to which the University is subject to (for example, certain laws require the University to keep records of your transactions for a certain period of time before we can delete them); or
- Whether retention is advisable in light of our legal position (such as in regard to applicable statutes of limitations, litigation or regulatory investigations).

Jurisdiction and Cross-Border Transfer

Your personal data will be stored and processed in Kenya and will not be transferred outside Kenya unless the provision of Section 25 (f) of the Data Protection Act is complied with i.e your consent is obtained or there is proof of adequate data protection safeguards and that the country whose data is to be transferred to has data protection laws equal to the Data Protection Act 2019 and authorization is obtained from the Office of the Data Protection Commissioner. In certain circumstances, courts, law enforcement agencies, regulatory agencies or security authorities in those other countries may be entitled to access your personal data subject to compliance with the provisions of treaties and conventions ratified by Kenya on Data Protection as well as the Data Protection Act, 2019.

Third-Party Payment Service

The University may use a third-party payment service to process payments made through the Services. If you wish to make a payment through the University Services, your personal data will be collected by such a third party and not by the University and will be subject to the third party's privacy policy, rather than this Privacy Policy. We have no control over and are not responsible for this third party's collection, use and disclosure of your Personal Information.

Contacting Us

The University of Nairobi is responsible for the collection, use and disclosure of personal data under this Privacy Statement. If you have any questions about this Privacy Statement, please contact us at **vc@uonbi.ac.ke** or:

Vice Chancellor
P.O. Box 30197-00100
Main Campus, Nairobi
Tel: +254 20 491 3614

Because email communications are not always secure, please do not include credit card or other sensitive information in your emails to us.

Additional Information

In accordance with applicable law, you may lodge a complaint with the Data Protection Commissioner's office.

Last Updated: May 2023

ANNEX 2

UNIVERSITY OF NAIROBI

Staff Privacy Statement

The University of Nairobi is aware of its obligations under the Kenya Data Protection Act (2019) and is committed to processing your data securely and transparently. This privacy notice sets out, in line with the Data Protection Act 2019, the types of data that we hold on you as an employee of the University. It also sets out how the University will use that information, how long the information will be kept and other relevant information about your data.

This notice applies to current and former employees, workers and contractors.

Data controller details

The University is a data controller, meaning that it determines the processes to be used when using your personal data. Our contact details are as follows: [University of Nairobi, P.O. Box 30197, GPO, Nairobi, Kenya; Tel: (+254-20) 491 0000]

Data protection principles

In relation to your personal data, the University will:

- Process it fairly, lawfully and in a clear, transparent way
- Collect your data for the reasons the University finds proper for the course of your employment in ways that have been explained to you
- Collect your data pursuant to any law provided that prior to the collection of such data, an explanation shall be availed to you.
- Only use it in the way that the University has explicitly told you about
- Ensure it is correct and up to date
- Keep your data for only as long as it shall be needed
- Process it in a way that ensures it will not be used for anything that you are not aware of or have consented to (as appropriate), except what is covered by the Act as exemptions.

Types of data the University will process

The University shall hold the following data about you;

- Your personal details including your name, address, date of birth, email address, phone numbers
- Gender
- Marital status
- Signatures
- Biological identifiers
- Personal data images
- Dependants, next of kin and their contact numbers
- Medical or health information including whether or not you have a disability
- Information used for equal opportunities monitoring about your religion or beliefs and ethnic origin
- Information included on your CV including references, education history and employment history
- Documentation relating to your right to work in Kenya
- Bank details
- KRA Tax Pin
- National Hospital Insurance Fund Number
- Current and previous job titles, job descriptions, pay grades, pension entitlement, hours of work and other terms and conditions relating to your employment with us
- Formal warnings and other documentation with regard to any disciplinary proceedings
- Internal performance information including measurements against targets, formal warnings and related documentation with regard to appraisal forms
- Leave records including annual leave, compassionate leave, sickness, leave of absence etc.
- Training details

How data will be collected

The University shall collect data about you in a variety of ways. The initial collection of your personal data will be during a recruitment exercise where you directly provide the data. This includes the information you would normally include in a CV or a recruitment cover letter, or notes made by our recruiting officers during a recruitment interview. Further information will be collected directly from you again, when you complete forms at the start of your employment, for example, your bank and next of kin details. Other details may be collected directly from you in the form of official documentation such as your passport or other right-to-work evidence.

In some instances, the University will collect data about you from third parties, such as former employers when gathering references or credit reference bureaus.

Personal data shall be stored manually in physical personnel files or electronically within the University's human resource information systems.

Why process your data?

The Data Protection Act, 2019 allows the processing of your data for the following reasons

only:

- In order to perform the employment contract that we are party to
- In order to carry out legally required duties
- In order to carry out legitimate interests
- To protect your interests and
- Where the processing is in public interest.

All of the personal data processing carried will fall under any one of the permitted reasons. For example, the University shall need to process your personal data in order to:

- Carry out the employment contract that entered into with you and
- Ensure you are paid.

Your data shall also be processed in order to ensure compliance with legal requirements such as:

- Ensuring your statutory obligations are paid out, for example tax and National Hospital Insurance are paid
- Carrying out checks in relation to your right to work in Kenya and
- Making reasonable adjustments for disabled employees.

Other legitimate reasons for the University to process your data are:

- Making decisions about who to offer initial employment to, and subsequent internal appointments, promotions etc.
- Making decisions about salary and other benefits
- Providing contractual benefits to you
- Maintaining comprehensive up to date personnel records about you to ensure, amongst other things, effective correspondence can be achieved and appropriate contact points in the event of an emergency are maintained
- Effectively monitoring both your conduct and your performance and to undertake procedures with regard to both of these if the need arises
- Offering a method of recourse for you against decisions made about you via a grievance procedure
- Assessing training needs
- Implementing an effective sickness absence management system including monitoring the amount of leave and subsequent actions to be taken including the making of reasonable adjustments
- Gaining expert medical opinion when making decisions about your fitness for work
- Managing statutory leave and pay systems such as maternity leave and pay etc.
- Dealing with legal claims
- Preventing fraud
- Ensuring our administrative and ICT systems are secure and robust against unauthorized access

Special categories of data

Special categories of data are data relating to your:

- Health
- Race
- Ethnic origin
- Biometric data
- Religion
- Conscience
- Belief
- Genetic data
- Property details
- Marital status
- Family details including names of your children, parents, spouse or spouses
- Sex or your sexual orientation

The University shall process special categories of data in accordance with more stringent guidelines. These special categories of data shall be processed when the following applies:

- You have given explicit consent to the processing
- Processing the data in order to carry out our legal obligations
- Process data for reasons of substantial public interest
- You have already made the data public.

The University shall also process your special category data:

- For the purposes of equal opportunities monitoring
- In sickness absence management procedures
- To determine reasonable adjustments

Although consent may not be needed in order to process the special categories of personal data in order to carry out legal obligations or exercise specific rights under employment law, consent will be sought when the University is called upon to process particularly sensitive data. If this occurs, you will be made fully aware of the reasons for the processing. As with all cases of seeking consent from you, you will have full control over your decision to give or withhold consent and there will be no consequences where consent is withheld.

Consent, once given, can be withdrawn at any time with no consequences.

If you do not provide your data to us

Should you not provide us with the personal data that is needed for the University to carry out its legal obligation expected under your contract of employment, the University will subsequently be unable to perform the said duties for example. ensuring you are paid correctly. The University may also be prevented from confirming, or continuing with, your employment in relation to the legal obligations if you do not provide this information e.g. confirming your right to work in Kenya or, where appropriate, confirming your legal status for carrying out your work via a criminal records check.

Sharing your data

Your data will be shared with colleagues within the University where it is necessary for them to undertake their duties. This includes, for example, your immediate supervisor for their management of you, the personnel department for maintaining personnel records and the finance department for administering payment under your contract of employment.

The University will share your data with third parties in order to meet regulatory obligations such as statutory remittances to KRA, obligations to Disclose, Deduct and Discharge payments to HELB or for other reasons to comply with a legal obligation upon us.

The University does not share your data with bodies outside Kenya.

Protecting your data

The University fully protects your data against accidental loss or disclosure, destruction and abuse by implementing both organizational and technical security measures.

Data shared with third parties is in line with requirements in the Data Protection Act, 2019 and the third parties must also implement appropriate technical and organizational measures to ensure the security of your data.

How long the University keeps your data

Your personal data will be retained only for as long as may be reasonably necessary to satisfy the purpose for which it is processed and following the data retention guidelines in the University's Records Management Policy.

Automated decision making

No decision will be made about you solely on the basis of automated decision making (where a decision is taken about you using an electronic system without human involvement) which has a significant impact on you.

Your rights in relation to your data

The Data Protection Act, 2019 has prescribed the following rights to you as the data owner:

- The right to be informed. This means that the University must tell you how your data is used and this is the purpose of this privacy notice
- The right to access. You have the right to access your data. Access to records and information shall be provided within the existing University regulatory framework
- The right for any inaccuracies to be corrected. If any data held about you is incomplete

or inaccurate, you are able to have it corrected

- The right to have information deleted. If you would like to stop processing your data, you have the right to ask for deletion from our systems where you believe there is no reason for the University to continue processing it
- The right to restrict the processing of the data. For example, if you believe the your data is incorrect, the University will stop processing the data (whilst still holding it) until the data has been corrected
- The right to portability. You may transfer the data about you for your own purposes
- The right to object to the inclusion of any information. You have the right to object to the way your data is used where the University may be using it for its legitimate interests

Where you have provided consent to the use of your data, you also have the unrestricted right to withdraw that consent at any time. Withdrawing your consent means that the University will stop processing the data that you had previously consent to use. There will be no consequences for withdrawing your consent.

If you wish to exercise any of the rights explained above, please contact the **VC's office.**

Making a complaint

The supervisory authority in Kenya for data protection matters is the Data Commissioner (DC). If you think your data protection rights have been breached in any way by us, you are able to make a complaint to the Data Commissioner's office.

ANNEX 3: SAMPLE CONSENT FORM

UNIVERSITY OF NAIROBI

STUDENT CONSENT FORM

I, _____ of registration number _____ hereby give consent to the University of Nairobi to use photographs or other images of me for marketing and branding purposes. I understand that these images may be used in print materials, on the university website, on social media platforms, or in other forms of marketing and promotional materials.

I acknowledge that UoN has the right to crop, edit, enhance, or modify these images as necessary for use in marketing and branding materials. I understand that my name may be used in connection with these images, but that the university will not release any personal information or contact details without obtaining additional consent.

I acknowledge that I will not receive any compensation for the use of these images and that the university will not be required to seek my approval for any subsequent use of these images.

I understand that I may revoke this consent at any time by providing written notice to the UoN Directorate of Corporate Affairs.

By signing this consent form, I confirm that I am 18 years of age or older, or that I have obtained the necessary consent from my parents or legal guardian.

If the individual is a minor, then I hereby give my permission on their behalf as their parent or legal guardian.

Name _____

Signature _____

Date _____

Minor's Name if Parent or Legal Guardian signed above on behalf of minor.

Student Name: _____