UNIVERSITIES FUND

DATA PROTECTION, PRIVACY AND RETENTION POLICY

MAY, 2023

UNIVERSITIES FUND

DATA PROTECTION, PRIVACY AND RETENTION POLICY

MAY 2023

Original Issue Date	
Last Reviewed Date	N/A
Effective Implementation Date	
Next review date	30th June 2024
Approver	The Universities Fund Board
Owner	Chief Executive Officer
Contact Person	
Classification	
Functional Applicability	UF
Consequences of grants Policy Breaches	Corrective Action
Version	UF Resource Mobilization Policy Version 1.0
Document Storage	UF Offices
Approved Minute	

TABLE OF CONTENTS

CHAPTER 1: DATA PROTECTION

DEFINITION OF TERMS

Consent means any freely given, unambiguous and informed indication by a statement or by a clear positive action, signifying an agreement by the user to the processing of his/her personal data.

Data controller means an individual person or company, public authority, agency or other body which has authority to oversee the management of, and to determine the purposes for the processing of personal data.

Data breach means the loss of, unauthorised access to, or unauthorised disclosure of the data.

Data processor means an individual person or company, public authority, agency or other body which processes personal data on behalf of the data controller.

Data processing means converting data into information. This includes collecting, recording, rationalizing, storage, alteration, retrieval, use, transmission, dissemination, erasure or destruction of data.

Data subject means an individual whose personal data is subject to processing.

Data transfer means all acts that make personal data accessible to third parties outside of the UF on paper, via electronic means, on the internet or through other means.

Data Transfer Agreement means an agreement between the UF and a third party that states the terms and conditions of use of personal data, including which data components are to be shared, the mode of transfer, how the data may be used, data security measures and other related issues.

Personal data means any data related to a user who can be identified from that data and other information; or by means reasonably likely to be used in relation to that data. Personal data includes biographical data (bio data) such as name, sex, date of birth, country of origin, Identification Number as well as blood type.

Personal data breach means a breach of data security leading to the accidental or unlawful/illegitimate destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transferred, stored or otherwise processed.

Person of concern means a person whose protection and assistance needs are of interest to the UF.

Processing of personal data means any operation, or set of operations, automated or not, which is performed on personal data, including but not limited to the collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, transfer, dissemination or otherwise making available, correction, or destruction.

Third party means an individual person or company other than the user. Examples of third parties are national governments, international governmental or non-governmental organizations, private sector entities or individuals.

ABBREVIATIONS

CI	Confidential Information
DPO	Data Protection Officer
EU	European Union
GDPR	General Data Protection Regulations
ICT	Information Communication and Technology
ID	Identification Document
IPRS	Integrated Population Registration System
KRA	Kenya Revenue Authority
MOU	Memorandum of Understanding
UF	Universities Fund

POLICY STATEMENT

The UF is committed to complying with all relevant Kenyan legislation and applicable global legislations. UF recognises that the protection of individuals through lawful, legitimate, and responsible processing and use of their personal data is a fundamental human right.

Under current legislation on data protection, it is a requirement to have a Data Protection Policy which should be regularly reviewed. In this regard, the Universities Fund strives to comply with the principles and obligations of Data Protection stated in the Kenya Data Protection Act, No. 24 of 2019 through the development of a Data Protection Policy.

This Data Protection Policy is a commitment of how the UF shall treat information of employees, customers, stakeholders and other interested parties with utmost care and confidentiality. The UF shall ensure that it protects the rights of data subjects and that the data it collects and processes is done in line with the required legislation. UF staff must comply with this policy, breach of which could result in disciplinary action.

INTRODUCTION

Recent concerns about the security of personal data stored in institutions have led to Governments enacting data protection regulations. In 2018, the European Union (EU) operationalised the General Data Protection Regulations (GDPR) that govern how companies handle personal data. Consequently, in 2019, Kenya enacted its own Data Protection Act. The regulations seek to protect the privacy of individuals by enforcing responsible processing of personal data. This includes embedding principles of lawful processing, minimising the collection of data, ensuring the accuracy of data and adopting security safeguards to protect personal data.

The Universities Fund has hence adopted the use of a data protection policy which provides a framework for safeguarding stakeholder's data from unauthorized access, use, disclosure, disruption, modification or destruction. This policy outlines the principles, guidelines and procedures that will be followed to ensure the confidentiality, integrity and availability of organizational information.

This data protection policy is designed to help everyone in any organization to understand their roles and responsibilities when it comes to protecting its stakeholders' data. It also defines the procedures that must be followed in the event of a data breach. By following this policy, the UF can minimize the risk of information threats and help to ensure that information is secure.

PURPOSE

The purpose of this policy is to provide guidelines relating to the processing of personal data by the Universities Fund (hereinafter referred to as "the UF"). It helps the UF comply with the data protection law, protect the rights of the data subjects and protect the UF from risks related to breaches of data protection.

SCOPE

This policy covers data collected, received and stored on the UF owned physical and electronic databases and resource centre. It shall apply to all staff, volunteers and members of the Board. It shall also apply to all users of the UF's applications, software, databases, websites, social media platforms and all other suchlike resources.

This policy shall cover all data/ information collection tools of the UF including but not being limited to assessment tools, databases, mobile applications, research publications and communication tools such as photos, videos, social and mainstream media.

1. Policy guidelines

This Data Protection Policy comprises the internationally accepted data privacy principles without replacing the existing national laws. It supplements the national data privacy laws.

The relevant national law will take precedence in the event that it conflicts with this Data Protection Policy, or it has stricter requirements than this Policy. The reporting requirements for data processing under national laws must be observed.

1.1 The UF shall, in dealing with personal information and data, ensure that the information/ data is processed;
- (a) without infringing the privacy rights of the data subject;
- (b) in a lawful manner; and
- (c) in a reasonable manner.

1.2 The collection, use, storage and transfer of personal data shall only be done in a manner guided by the fundamental principles of the UF.

1.3 This policy shall guide the UF's ICT Policies and the Records Management Policy.

2. Accuracy

2.1 The UF shall store personal data/information as accurately as possible, update and systematically review it to ensure it fulfils the purpose(s) for which it is processed.

2.2 The data subject may request the correction of personal data that is inaccurate, incomplete, unnecessary or excessive.

2.3 When personal data is corrected, the UF shall notify, as soon as is reasonably practicable, all third parties to whom the relevant personal data was transferred and to the data subject.

2.4 Personal data on file must be correct, complete and be kept up to date. Suitable steps must be taken by the UF DPO to ensure that inaccurate or incomplete data is deleted, corrected, supplemented or updated.

3. Data protection officer

3.1 The UF has designated the Head of ICT department to be the Data Protection Officer (DPO). Accordingly, the DPO shall:

(a) Advise the UF staff on requirements for data protection, including data protection impact assessments.

(b) Ensure that the UF has complied with the legal requirements on data protection.

(c) Facilitate capacity building of staff involved in data processing operations.

(d) Cooperate with external regulators on matters relating to data protection.

(e) Monitor and evaluate the efficiency of the data systems in the UF and keeping written records of the processing activities of the civil registration entity.

(f) Facilitate in investigation of data breaches and other infringements.

UF DPO can be contacted via the email:*data.protection@ufb.go.ke*

4. Duty to notify

4.1 The UF has a duty to notify data subjects of their rights before processing data. UF shall therefore inform the data subjects of their right:

(a) To be informed of the use to which their personal data is to be put.

(b) To access their personal data in UF custody.

(c) To object to the processing of all or part of their personal data.
(d) To the correction of false or misleading data.
(e) To delete false or misleading data about them.

5. Lawful and fair processing

5.1 Data processing shall be carried out in a lawful and fair manner for specified and legitimate purposes without prejudicing the fundamental rights and freedoms of data subjects.

5.2 The processing shall only be justified based on one (or more) of the legal basis including:

(a) data subject giving his or her consent.
(b) the processing is necessary for the performance of a contract with the data subject.
(c) to meet legal compliance obligations.
(d) to protect the data subject's vital interests or any other person who may be indirectly affected
(e) public interest
(f) to pursue the UF's legitimate interests which are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects.

6. Further processing

6.1 Further processing for research purposes shall be compliant with the conditions as outlined in this policy.

6.2 Personal data which is processed for research purposes may be exempted from the provisions of this policy if the results of the research and statistical data is not made available in a form which identifies the data subject.

6.3 Further processing of data shall comply with the data protection principles set out in this policy, in particular, ensuring the security and confidentiality of sensitive personal data.

7. Principles for Processing Personal Data

7.1 Fairness and Lawfulness; When processing personal data, the individual rights of the data subjects must be protected. Personal data must be collected and processed in a legal and fair manner. Collected data shall be adequate, relevant and not excessive in relation to the purposes for which it is obtained and their further processing. Individual data can be processed upon voluntary consent of the person concerned.

7.2 Restriction to a specific purpose; Personal data can be processed only for the purpose that was defined before the data was collected. Personal data shall be obtained for specified, explicit and legitimate purposes, and shall not subsequently be processed in a manner that is incompatible.

7.3 Confidentiality and Data Security; Personal data is subject to data secrecy. It must be treated as confidential on a personal level and secured with suitable organisational and technical measures to prevent unauthorised access, illegal processing or distribution, as well as accidental loss, modification or destruction.

8. Confidentiality

8.1 The confidentiality of personal data must be respected by the UF when processing data at all times with access to the same limited on a need to know basis.

8.2 The UF shall maintain the confidentiality of the personal data throughout and even after the user is no longer of concern to the UF.

8.3 Health data will be kept separate from other personal data and will be accessible by healthcare providers or specific personnel employed to manage health data by the UF under confidentiality guarantees.

8.4 The UF may specify other categories of personal data that will require additional safeguards and restrictions and may be classified as sensitive personal data.

8.5 In the processing of sensitive personal data, the UF will specify further grounds on which these categories will be processed with consideration of:

(a) the increased risk of significant harm that may be caused to the data subject by processing this category of personal data.

(b) the degree of confidentiality attached to the category of personal data.

(c) the level of protection afforded by provisions applicable to personal data.

8.6 The UF shall process personal data of children in a manner that protects their rights and best interests.

8.7 The UF shal incorporate a process of obtaining parental consent and age verification in order to process personal data of children.

9. Security

9.1 The UF shall ensure and implement a high level of data security that is appropriate to the risks presented by the nature and processing of personal data taking into account the level of technology available and existing security conditions as well as the costs of implementing additional security measures.

9.2 In order to ensure and respect confidentiality, personal data shall be filed and stored in a way that is accessible only to authorized staff and transferred only through the use of protected means of communication.

9.3 In order to ensure the confidentiality of the personal data, the UF shall take appropriate technical and organizational data security measures.

9.4 The nature of risks shall include but not be limited to

risk of accidental or unlawful/illegitimate destruction, loss, alteration, unauthorized disclosure of or access to personal data.

9.5 Access to personal data/content/knowledge shall be restricted to authorized personnel using it in the performance of their duties at the UF and as determined by appropriate authorization of both the staff or volunteers' supervisor and data subjects.

9.6 Personal data/content/knowledge may not be used by any employee or staff for purposes other than the business of the UF.

9.7 Staff and volunteers allowed access to personal data/ content/knowledge of the UF shall sign a nondisclosure agreement banning them from using the content for business other than the UF's core mandate.

9.8 Private email accounts shall not be used to transfer Personal Data.

9.9 Information technology shall be used to process, communicate and store UF data and information which will be classified as Confidential Information (CI).

9.10 Data security measures shall be routinely reviewed and upgraded as deemed appropriate to ensure the level of protection is commensurate to the degree of sensitivity applied to personal data and considering the possible development of new technology in enhancing data security.

10. Accountability

10.1 The UF shall be responsible for compliance and shall be required to demonstrate that appropriate measures have been employed within the organization to comply with the data protection guidelines.

10.2 The UF shall implement data protection training programmes for all staff.

10.3 The UF shall bear the burden of proof to establish the data subjects' consent of the processing of their personal data for a specific purpose.

10.4 The UF shall ensure that it is as easy to withdraw as it is to give consent.

11. Rights of data subjects

11.1 A data subject has a right to;

(a) be informed of the use to which their personal data is to be put.

(b) withdraw consent at any time.

(c) access their personal data in custody of the UF or data processor.

(d) object to the processing of all or part of their personal data.

(e) correction of false, inaccurate or misleading data about them.

(f) deletion of false or misleading data about them.

(g) request for erasure of their personal data where it is irrelevant, excessive or was obtained unlawfully.

12. Data collection

12.1 When collecting personal data from the user, the UF shall inform the user of the following in writing/orally and in a manner and language that is understandable to the user:

(a) The specific purpose(s) for which the personal data or categories of personal data will be processed.

(b) Whether such data will be transferred to third parties and the specific third parties.

(c) The data subject's right to request access to their personal data, or correction or deletion of it.

(d) How to lodge a complaint with the UF.

(e) The mandate and contact details of the UF.

10.2 Where data is not collected directly from the data subject either orally or in writing, other means will be considered as far as is practicable such as radio communication, posters and flyers in an accessible location, online postings and any other appropriate method of transmission.

10.3 At the request of the data subject, the UF may restrict the processing of personal data where:

(a) The accuracy of the data is contested by the data subject.

(b) The data subject has objected to the processing.

13. Data Mining

13.1 The UF shall involve and consult data subjects and other stakeholders in the design and implementation of data mining standards and guidelines.

13.2 A privacy-by-default and privacy-by-design approach shall be adopted, and data mining privacy techniques and tools shall be tailored to the specific context and purpose.

13.3 Data mining privacy policies and standards shall be reviewed regularly in order to adapt them to the changing legal, technological and social landscape.

13.4 A culture of data mining privacy shall be established within the UF, with training and guidance provided to data miners and users on appropriate principles and practices.

14. Data Protection Impact Assessments

14.1 Where a type of processing in particular using new technology, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the UF shall, prior to the processing, carry out

an assessment of the impact of the envisaged processing operations on the protection of personal data.

14.2 A single assessment may address a set of similar processing operations that present similar high risks.

14.3 A data protection impact assessment shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; or

(b) a systematic monitoring of a publicly accessible area on a large scale.

14.4 The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the UF;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Policy taking into account the rights and legitimate interests of data subjects and other persons concerned.

15. Processing sensitive personal data

15.1 The UF shall process sensitive personal data only when:

(a) The processing is carried out in the course of legitimate activities with appropriate safeguards and that the processing relates solely to the staff or to persons who have regular contact with UF and the personal data is not disclosed outside UF without the consent of the data subject.

(b) The processing relates to personal data that has been made public by the data subject.

(c) Processing is necessary for:

(i) The establishment, exercise or defence of a legal claim.

(ii) The purpose of carrying out the obligations and exercising specific rights of the UF or of the data subject.

(iii) Protecting the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent.

16. Transfer of personal data to third parties

16.1 The UF may only transfer personal data/content/ knowledge to third parties on condition that the third party affords a level of data protection that is the same or comparable to this Policy.

16.2 In order to mitigate risks associated with transfer of data to third parties, the UF will only transfer data to a third party if:

(a) The data is stripped off personal and identifiable information;

(b) The transfer is based on one or more legitimate basis including:

(i) explicit consent by the data subject;

(ii) compliance with national or international law; or

(iii) in exercise, establishment and defense of any contractual or legal obligations.

(c) The personal data to be transferred is adequate, relevant, necessary and not excessive in relation to the purpose(s) for which it is being transferred;

(d) The data subject has been informed either at the time of the collection or subsequently, about the potential transfer of his/her personal data;

(e) The third party has in the past respected the confidentiality of personal data transferred to them by the UF; and

(f) The third party maintains a high level of data security that protects personal data against the risk of accidental or unlawful/illegitimate destruction, loss, alteration, unauthorized disclosure of, or access to it.

16.3 The UF shall also ensure that transferring personal data does not negatively impact:

(a) The safety and security of the UF staff, volunteers and beneficiaries.

(b) The effective functioning of an operation or compromise in the UF's mission, vision or fundamental principles, for example due to the loss of trust and confidence between the UF and persons of concern.

16.4 The processing of sensitive personal data out of Kenya shall only be effected upon obtaining consent of a data subject and on obtaining confirmation of appropriate safeguards.

17. Data transfer records

17.1 The UF shall keep and maintain full and accurate records reflecting all phases of data management cycle, including records of data subjects' consents and procedures for obtaining consent, where consent is the legal basis of processing.

17.2 The data transfer records shall include, at a minimum:

(a) the name and contact details of the individual entity authorizing the transfer;
(b) clear descriptions of the personal data types;
(c) data subject types;
(d) processing activities;
(e) processing purposes;
(f) third-party recipients of the personal data;
(g) personal data storage locations;
(h) personal data transfers;
(i) the personal data's retention period; and
(j) a description of the security measures in place.

18. Data transfer agreements

18.1 The UF will require all third parties to comply with this Policy through an agreement or an MOU as part of the signing of partnership agreements. Such agreements will specify the specific purpose(s) and legitimate basis for the processing or transfer of personal data.

18.2 Data transfer agreements shall;

(a) address the purpose(s) for data transfer, specific data elements to be transferred as well as data protection and data security measures to be put in place;
(b) require the third party to undertake that its data protection and data security measures are in compliance with this Policy; and

(c) stimulate consultation, supervision, accountability and review mechanisms for the oversight of the transfer for the life of the agreement.

18.3 The Legal Department of the UF shall review and approve all data transfer agreements and maintain copies of final agreements.

19. External use and legal provisions

19.1 Title to all data belonging to the UF resulting from data processing shall reside in the UF and shall be protected by data protection laws of the Country.

19.2 Third parties may not process data belonging to the UF without consultation with the UF.

19.3 Any data processed jointly shall be jointly owned by the UF and third the party with whom the joint processing was done.

19.4 Nothing in this policy will prevent legal action from being undertaken against a person who violates the provisions of this policy or of any Kenyan laws and regulations.

19.5 All matters arising out of or relating to this policy shall be governed by and are to be construed in accordance with the Laws of Kenya, excluding any conflict of law provisions, with Kenyan courts having exclusive jurisdiction in all disputes arising therein.

CHAPTER 2: DATA PRIVACY

1. Introduction

The Universities Fund recognizes privacy rights as guaranteed under the Data Protection Laws and Regulations. Thus, it is important that personal data is managed, processed and protected in accordance with the provisions of the applicable laws. In the course of UF business with relevant stakeholders through UF platforms (this includes but is not limited to our websites, digital platforms, mobile applications, physical operations/ offices, amongst others), the UF shall process personal data, subject to the terms of this Policy.

2. Collection of Information

The UF collects **"Non-Personal Information"** and "**Personal Information**." **Non-Personal Information** includes information that cannot be used to personally identify individuals, such as anonymous usage data, general demographic information may be collected, referring/exit pages and URLs, platform types, preferences you submit and preferences that are generated based on the data you submit and number of clicks. **Personal Information** includes individual(s) email, National ID Number/Passport Number/Allien ID, Date of Birth, Address, Phone Number, Profession, Bank Account, Citizenship, Source of Income, which is submitted to UF when using the Fund's systems.

3. Information Collected

In the course of UF's engagement with stakeholders through UF Platforms, personal data may be collected in the following ways:

3.1 **Automatic information collection:** the UF may automatically collect information upon engagement with stakeholders through computers, mobile phones, forms, documents made available to the UF and other

access devices like a webservice call. The UF may also collect anonymous information through use of cookies and web beacons to customize stakeholders' experience of UF's platform and to improve account security. Stakeholders may decline UF use of cookies, unless the same is mandatory for the use of UF platform. Please note that refusal to permit the use of cookies may affect stakeholders' use of UF's platform.

3.2 **Information from downloads:** When stakeholders download or use UF's digital platforms, or access any of UF's sites, the UF may receive information about stakeholders' location and mobile device, including a unique identifier for their device. The UF may use this information to provide stakeholders with location-based services, such as search results and other personalized content. Stakeholders may disable their location in the settings menu of the device.

3.3 **Physically or digitally provided information**: The UF shall collect and process stakeholders' information upon creation and/or updating of accounts on UF's platform; complete forms, questionnaires, surveys etc. The UF shall also collect information from the data provided through documents, letters, e-mail, agreements, correspondence, ID cards, passports, or through any other means which stakeholders wilfully provide information to the UF.

3.4 **Third Parties**: The UF may also receive your information from third parties such as guardians, financial institutions, KRA, IPRS and other sources.

4.5 **Social Media:** The UF shall also receive information through stakeholder engagements with the UF on social media sites (e.g., Facebook, Instagram, LinkedIn, Twitter and WhatsApp). This includes but is not limited to stakeholder replies to UF posts, comments, enquiries, messages to the UF, etc.

4. Use and sharing of Information

4.1 The UF shall collect personal and non-personal information about stakeholders during the course of interactions with the UF or through UF platforms for a variety of legal reasons, primarily so that the UF may customize stakeholders experience and give better service. The UF collects information in order to:

(a) provide services and customer support;

(b) process transactions, payment requests and send notices about transactions;

(c) create an account with the UF for the provision or use of UF services;

(d) verify customers' identity, including during account creation and password reset processes;

(e) manage customer accounts and provide them with efficient customer service,

(f) resolve disputes, process payments and troubleshoot problems;

(g) manage risks, or detect, prevent, and/or remediate fraud, violation of policies and applicable user agreements or other potentially prohibited or illegal activities;

(h) execute UF's legal and contractual obligations to stakeholders;

(i) improve UF's services and functionality by customizing user experience;

(j) measure the performance of UF's services and improve their content and layout;

(k) manage and protect UF's information technology infrastructure;

(l) obtain a means by which the UF may contact stakeholders; either by telephone, text (SMS), email messaging, social media, etc;

(m) conduct background checks, compare information for accuracy and verify the same with third parties;
(n) identify or address a violation and administer UF's policies and terms of use;
(o) comply with legal, contractual and regulatory obligations;
(p) execute stakeholders' specific requests or use the same for a specific purpose as instructed;
(q) investigate and respond to stakeholder complaints or enquiries;
(r) process stakeholders' access to UF's services, platforms or functions from time to time;

4.2 If the UF intends to use any personal information in any manner that is not consistent with this policy, stakeholders will be informed of such anticipated use prior to or at the time at which the personal information is required and obtain consent.

4.3 Except as otherwise stated in this policy and other statutory provisions or laws enacted by the parliament of Kenya, UF does not sell, trade, rent or otherwise share personal Information with third parties without your consent.

5. Training and Compliance

5.1 UF provides regular training and awareness programmes to employees, contractors and volunteers on data privacy principles, practices and their responsibilities.

5.2 Compliance with this policy is mandatory for all individuals accessing or processing personal data on behalf of the UF.

CHAPTER 3: DATA RETENTION

1. Introduction

1.1 Data retention outlines the principles and guidelines for the retention, storage and disposal of data collected, processed, and stored by UF.

2. Purpose

2.1 The purpose is to ensure that necessary data is adequately protected and maintained, while also ensuring that data no longer needed is properly disposed of in a timely and secure manner. This applies to all employees, contractors and third-party service providers who handle data on behalf of the UF. It covers all types of data, including electronic and physical records, as well as any other forms of data storage.

2.2 Data will not be kept in a form that allows data subjects to be identified for longer than needed for the legitimate UF's purposes or other purposes for which the UF collected it. The purposes of data retention shall include satisfying any legal, contractual, accounting or reporting requirements. Personal data may be retained for a longer period in the event of a complaint where there is reasonable belief that there is a prospect of litigation in respect to the UF's relationship with the data subject.

3. Data Classification

3.1 To ensure that data is retained for the appropriate length of time, all data shall be classified according to its sensitivity and importance to the UF.

3.2 Data shall be categorized into the classifications as defined in the UF's Information Security Policy.

4. Data Retention Periods

4.1 The retention period for data provided under this policy takes into consideration:classification of data, contractual obligations, the purpose of data and the requirements of the law. Where it is not possible to define a statutory or legal retention period in line with the applicable data protection/privacy laws, the UF shall identify the criteria by which the period can be determined (such as industry standards) and update this Policy as may be necessary.

4.2 Records must be categorised by purpose and retained for specific periods in accordance with the Retention Schedule below. Retained Records will be grouped by category and in a clear date order when the Record was stored and/or archived.

4.3 Notwithstanding the retention periods provided in the retention schedule below, Records which are subject of, or required in any pending litigation, investigation or other regulatory process shall not be destroyed or altered, until the completion of such process.

4.4 Data should be retained for the minimum amount of time necessary to fulfil its purpose. The following retention periods shall apply to each data classification:-

Confidential: Retain for a minimum of 7 years or as required by applicable laws and regulations.

Internal: Retain for a minimum of 3 years or as required by applicable laws and regulations.

Public: Retain for a minimum of 1 year or as required by applicable laws and regulations.

5. Storage and Security

5.1 All data must be stored in a secure m anner that protects it from unauthorized access, alteration or destruction. This includes:

(a) Ensuring that electronic data is stored on secure servers with appropriate access controls and encryption.

(b) Storing physical data in locked cabinets or secure storage areas.

(c) Regularly backing up data to prevent loss or corruption.

6. Data Disposal

6.1 When data has reached the end of its retention period, it must be securely disposed of in a manner that prevents unauthorized access or disclosure. This include:-

(a) Securely deleting electronic data using approved software or tools.

(b) Shredding or otherwise physically destroying paper records.

(c) Ensuring that third-party service providers who handle data disposal adhere to the same security standards as the UF.

6.2 The UF shall take all reasonable steps to destroy or erase from its systems all personal data that is no longer required.

7. Roles and Responsibilities

7.1 All employees, contractors, and third-party service providers are responsible for adhering to this Policy and ensuring that data is properly retained, stored and disposed of.

7.2 The UF's Data Protection Officer (DPO) is responsible for overseeing compliance with this Policy and providing guidance on data retention and disposal matters.

CHAPTER 4: DATA BREACH RESPONSE PLAN

1. Introduction

1.1 A data breach involves the loss of, unauthorised access to, or unauthorised disclosure of the data.

1.2 A data breach may occur through:

(a) The accidental loss or theft of data or information (including a hard copy)

(b) The transfer of sensitive or confidential information to those who are not authorized to receive that information.

c) Attempts (either failed or successful) to gain unauthorized access to data, information systems or a computing device.

d) Changes to information or data, system hardware, firmware or software configuration.

2. Purpose

2.1 The Data Breach Response Plan sets out the process to be followed by the UF staff in the event of a data breach.

3. Potential impacts of a data breach

3.1 The impact of a data breach depends on the nature and extent of the breach and the type of information that has been compromised. Serious impacts of a breach could include:

1. Risks to individuals' safety.
2. Financial loss to an individual or organization.
3. Damage to personal reputation or position.
4. Commercial risk through disclosure of commercially sensitive information to third parties.
5. Threat to systems, leading to disruption of activities.
6. Impact on Government reputation, finances, interests or operation.

3.2 It is important to note that breaches of personal data can result in significant harm, including people having their identity stolen or the private home addresses of vulnerable people being disclosed. As such, even a breach affecting an individual or a small number of people may have a large impact.

4. Process for responding to a data breach

4.1 The following steps outline the process which must be followed by the UF staff in relation to any breach incident, including a suspected but unconfirmed incident.

Step 1: Alert

Where a data breach is known to have occurred (or is suspected) any member of the UF staff who becomes aware of the breach must immediately alert the Data Protection Officer (DPO) and the UF Management.

Where possible, the staff member who discovered the breach should try and provide the following information:

- Contact name and number of persons reporting the incident.
- The type of data or information involved.
- Whether the loss of the data puts any person or other data at risk.
- Location of the incident.
- Date and time when the breach occurred.
- Location of data or equipment affected.
- Type and circumstances of the incident.

It is important to note that the staff member who discovered the breach should alert these teams immediately, and not wait until all the key details on the breach have been established.

If the staff member who discovers the breach is authorised by the UF to take action to contain the breach, they must act as soon as possible to contain the breach and minimise the damage. This may involve:

- shutting down of applications;
- closing of accounts;
- changing passwords;
- attempting to locate missing items or
- restricting access rights.

Please note that not all staff will be authorised to take these actions, and containment should only be enacted by authorised staff.

Step 2: Verification

Once notified of any data breach, the DPO and the relevant UF Management must quickly establish the key details of the breach, including when it occurred or was identified, how it occurred, what data was affected and the extent of the breach.

The DPO must also consider whether the data breach involves personal information and provide findings to the relevant UF Management.

Step 3: Impact Assessment

Impact assessment will be conducted where personal data has been accessed or acquired by an unauthorised person, and to establish if there is a real risk of harm to the data subject whose personal data has been subjected to the unauthorised access.

The DPO is then responsible for determining the seriousness of the data breach. While there is no objective measure of seriousness, the DPO will need to work out what constitutes a serious breach by considering:

- The type of data held
- Whether personal information was disclosed such as; full name, identification number, an account name, account number, any

password, security code, access code, response to a security question, biometric data or other data that is used or required to allow access to or use of the individual's account
- The number of individuals affected
- The risk of harm that could be caused to both individuals and the UF by the breach.

In assessing the seriousness of the breach, the DPO will need to consider:
- The type of data that has been breached – does it include financial, health or other sensitive categories of data? Are there other characteristics of the data that could pose a high risk (e.g. commercial information that could pose a reputational risk to another organisation?)
- The data context – does the breach affect data that would normally be publicly available, or is the data known to be very poor quality that if used could create risk to individuals?
- How easy would it be for individuals to be identified from this data?
- The circumstances of the breach – for example, was it a single incident (such as the loss of a laptop) or a malicious attack that poses an ongoing risk, or was the data altered in a way that it would pose a risk to the individuals to whom the data relates?

The responses to these questions, and assessment of the overall impact of the breach, are to be reported to the Head of Department affected, Head of ICT and the UF Management. The DPO is also responsible for logging the incident in the UF system for record management purposes.

Step 4: Rectification

The Head of the Department affected by the breach must take steps to eliminate the circumstances enabling the breach. The DPO shall record these steps in the UF system.

Step 5: Notification

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 UF Management shall—

1. Notify the Board of Trustees;
2. Notify the Data Commissioner without delay, within seventy-two hours of becoming aware of such breach; and
3. Communicate to the data subject in writing within a reasonably practical period, unless the identity of the data subject cannot be established.
4. Where the notification to the Data Commissioner is not made within seventy-two hours, the notification shall be accompanied by reasons for the delay.
5. The UF Management may delay or restrict notifying data subjects as necessary and proportionate for purposes of prevention, detection or investigation of an offence by the concerned relevant body.

A notification to the Data Commissioner of a notifiable data breach shall include—

(a) the date on which and the circumstances in which the UF Management first became aware that the data breach had occurred;

(b) a chronological account of the steps taken by the UF Management after it became aware that the data breach had occurred, including the DPO's assessment that the data breach is a notifiable data breach;

(c) details on how the notifiable data breach occurred, where applicable;

(d) the number of data subjects or other persons affected by the notifiable data breach;

(e) the personal data or classes of personal data affected by the notifiable data breach;

(f) the potential harm to the affected data subjects as a result of the notifiable data breach;

(g) information on any action by the UF Management, whether taken before or to be taken after it notifies the Data Commissioner of the occurrence of the notifiable data breach to—

(i) eliminate or mitigate any potential harm to any affected data subject or other person as a result of the notifiable data breach; or

(ii) address or remedy any failure or shortcoming that the UF Management believes to have caused, or enabled or facilitated the occurrence of, the notifiable data breach;

(iii) the affected individuals or the public that the notifiable data breach has occurred and how an affected data subject may eliminate or mitigate any potential harm as a result of the notifiable data breach; or

(iv) contact information of an authorized representative of the UF Management.

Step 6: Review

Once the matters referred have been dealt with, the DPO and the UF Management should identify lessons learn and remedial action that can be taken to reduce the likelihood of recurrence.

This might include a review and remediation of:

- The internal controls in place.
- Policies and procedures.
- Staff skills and refresher training.
- Contractual obligations with contracted service providers.

5. RACI

Process	Incident Identifier	DPO	Relevant Management (Department Affected)	UF Management	Head of Department affected	Board of Trustees	Data Subject	Data Commissioner
Alert	R	I	I	I	N/A	N/A	N/A	N/A
Verification	I	RA	C	I	N/A	N/A	N/A	N/A
Impact Assessment	I	C	RA	I	I	I	N/A	N/A
Rectification	C	C	RA	I	C	C	N/A	N/A
Notification	I	C	C	RA	I	I	I	I
Review	C	RA	RA	RA	RA	AC	I	N/A

The section below lists the responsibilities and roles of UF teams when a breach occurs or is suspected.

R: Responsible A: Accountable C: Consult I: Inform N/A: Not applicable

6. Evaluation and Review

Monitoring:	UF DPO will undertake ad hoc observations and audits of the Data Breach Response Plan.
Evaluation and review:	The Response Plan will be reviewed bi-annually or in the event of legislative or policy changes relating to data breach notifications.

7. Enforcement

7.1 Failure to comply with this Policy may result in disciplinary action, up to and including termination of employment or contract, as well as potential legal and financial consequences for the organization.

8. Periodic review of the knowledge management policy

8.1 This policy will be reviewed every three years or when need arises, whichever comes first.

Hazina Trade Centre, 5th Floor, Monrovia Street

P.O BOX 28237-00100,Nairobi Kenya

+254 207903331 / +254 746737935

info@ufb.go.ke