

FUNDILIMA SACCO SOCIETY LIMITED

Data Protection Policy

© 2022



TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS 4

DEFINITION OF TERMS 5

1.0 INTRODUCTION 8

1.1 PURPOSE OF THIS POLICY 8
1.2 SCOPE OF THIS POLICY 9
1.3 APPOINTMENT OF A DATA PROTECTION OFFICER 9
1.4 REGISTRATION WITH THE OFFICE OF THE DATA COMMISSIONER 9

2.0 DATA GOVERNANCE 10

2.1 FUNCTIONAL STRUCTURE 10
2.2 RESPONSIBILITIES 10
2.3 DATA COMMUNICATION 14
2.4 DATA CLEANSING 14
2.5 DATA CLASSIFICATION 15

3.0 PERSONAL INFORMATION MANAGEMENT 17

3.1 JUSTIFICATION FOR COLLECTING PERSONAL INFORMATION 17
3.2 SOURCES OF PERSONAL INFORMATION 17
3.3 FORMS OF PERSONAL INFORMATION COLLECTED 18
3.4 DATA SUBJECT CONSENT 19
3.5 CONFIDENTIALITY OF DATA PROCESSING 20
3.6 DATA PROCESSING SECURITY 20
3.7 DATA RETENTION POLICY 21

4.0 DATA PROTECTION AND PRIVACY 22

4.1 DATA PROTECTION PRINCIPLES 22

4.2 RIGHTS OF DATA SUBJECTS 24
4.3 NECESSITY IN DATA PROCESSING 25
4.4 DIRECT AND ELECTRONIC MARKETING 25
5.0 DATA BREACH RESPONSE PLAN 26
6.0 AUTOMATED DECISION MAKING 26
7.0 INFORMATION SHARING 26
8.0 CAPACITY BUILDING 27
9.0 COMPLIANCE 27
POLICY REVISION 28
ADOPTION OF POLICY 29
APPENDICES 30
APPENDIX 1: OATH OF SECRECY/ CONFIDENTIALITY 30
APPENDIX 2: THIRD PARTIES/ PARTNER NON-DISCLOSURE AGREEMENT 31

ABBREVIATIONS AND ACRONYMS

BOD	–	Board of Directors
CEO	–	Chief Executive Officer
CRB	–	Credit Reference Bureau
DPIA	–	Data Protection Impact Assessment
DPO	–	Data Protection Officer
EACC	–	Ethics and Anti-Corruption Commission
ICT	–	Information and Communication Technology
ID	–	Identification
NHIF	–	National Hospital Insurance Fund
NSSF	–	National Social Security Fund
SASRA	–	Sacco Societies Regulatory Authority
SLA	–	Service Level Agreement

DEFINITION OF TERMS

Anonymisation	The removal of personal identifiers from personal data so that the data subject is no longer identifiable.
Biometric data	Personal data resulting from specific technical processing based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, deoxyribonucleic acid analysis, earlobe geometry, retinal scanning and voice recognition.
Consent	Agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal data relating to them.
Data	Information that is processed using equipment operating automatically in response to instructions given for that purpose or recorded with the intention that it should be processed using such equipment or recorded as part of a relevant filing system.
Data Controller	The person or organisation that determines when, why and how to process personal data. It is responsible for establishing practices and policies under the Data Protection Act. Fundilima Sacco is the Data Controller of all personal data relating to it and used in facilitating its business operations.
Data Processing	Any activity that involves the use of personal data and includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties. In brief, it is anything that can be done to personal data from its creation to its destruction, including both creation and destruction.

Data Protection Impact Assessment	This is a tool or procedure for identifying and reducing risks involved in any processing activity that will involve personal data.
Data Protection Officer	The person appointed as such under the Data Protection Act following its requirements. A data protection officer is responsible for advising the Sacco (including employees) on their obligations under various data protection laws, for monitoring compliance with data protection law, as well as with Fundilima Sacco policies.
Data Subject	A living, identified or identifiable individual about whom the Sacco hold personal data.
Personal Data	Any information identifying a data subject or information relating to a data subject that the Sacco can identify (directly or indirectly) from that data alone or in combination with other identifiers the Sacco possess or can reasonably access. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour
Personal Data Breach	Any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data, where that breach results in a risk to the data subject.
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular, to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of automated processing.

Third-Party	Any natural or legal person other than the data subject, Fundilima Sacco, or any implementing partner.

1.0 INTRODUCTION

1.1 PURPOSE OF THIS POLICY

This Data Protection Policy has been developed as a guide to Fundilima Sacco in the management of stakeholders' data. Fundilima Sacco obtains, uses, stores and otherwise processes personal data relating to its stakeholders such as potential and current employees, former staff, members, suppliers, visitors to Sacco premises, contractors and website users, collectively referred to in this policy as data subjects. This Policy sets out how the Sacco manages those responsibilities.

In developing this Policy, the BOD intends to have this as the primary reference point for all matters on data protection in the Sacco. Contents of this Policy will therefore be carefully studied and implemented, as it constitutes an integral part of the Society's compliance and risk management processes. The Policy will be circulated to all Sacco employees to enable them to familiarise themselves with the provisions herein.

The Sacco heavily draws its data policy guidelines from the Data Protection Act, 2019 and the Data Protection General Regulations, 2021. When processing personal data, the Sacco is obliged to fulfil individuals' reasonable expectations of privacy by complying with the Act and related Regulations and other relevant data protection legislation.

The policy document is therefore intended to ensure that the Sacco:

- Is clear about how personal data must be processed and the Sacco's expectations for all those who process personal data on its behalf;
- Complies with existing data protection laws and with good practice;
- Protects its reputation by ensuring the personal data entrusted to it is processed per data subjects' rights;
- Protects itself from risks of personal data breaches and other breaches of data protection law.

1.2 Scope of this policy

This policy applies to all personal data the Sacco processes regardless of the location where that personal data is stored (e.g. on an employee's own device, Fundilima Sacco's servers, Sacco website, etc.) and regardless of the data subject. All staff and others processing personal data on Fundilima Sacco's behalf must read and comply with the provisions of this Policy. Failure to comply with this policy may result in disciplinary action.

1.3 Appointment of a Data Protection Officer

The Board of Directors shall from time to time appoint a suitably qualified employee to the role of a Data Protection Officer. This need not be a role performed exclusively but could be in addition to other roles played in the Sacco. Until otherwise determined, the ICT Manager shall also play the role of Data Protection Officer (DPO).

1.4 Registration with the Office of the Data Commissioner

The Sacco shall register with the Office of the Data Commissioner as a data controller and processor following the Data Protection Act and Regulations thereof.

2.0 DATA GOVERNANCE

2.1 FUNCTIONAL STRUCTURE

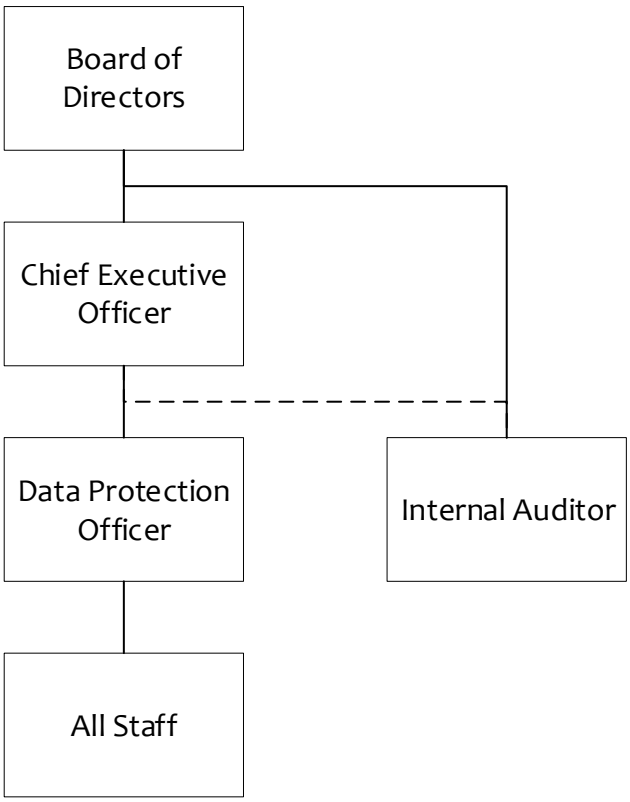


Figure 1: Data Governance Structure

2.2 RESPONSIBILITIES

2.2.1 Board of Directors

Under this policy, the Board of directors have the following responsibilities;

a) To regularly review and update this policy and its provisions ensuring that they comply with the applicable data protection laws;
b) To allocate adequate resources every year in the normal budgeting cycle to ensure achievement of the policy objectives; and
c) To appoint a suitably qualified individual into the role of Data Protection Officer.

2.2.2 Sacco Responsibilities as a Data Controller

a) The Sacco being a Data Controller shall undertake to carry out a Data Privacy Impact Assessment (DPIA) to identify and minimize risks involved in projects, processes and activities involving directly or indirectly processing of personal data;
b) The DPIA will be required for processing where there is a likelihood of high risk to individuals and their data and where new technologies are involved; and
c) The Data Protection Officer shall undertake the privacy assessment in assistance with the relevant department and sign off the reports;
d) Co-operate with the Data Commissioner and any other authority on matters relating to data protection.

2.2.3 Data Protection Officer Responsibilities

The Data Protection Officer is responsible for:

a) Advising the Sacco and its staff of its obligations under relevant data protection laws and regulations;
b) Monitoring compliance with this Policy and other relevant data protection laws, and monitoring training activities that relate to data protection compliance;
c) Providing advice where requested on data protection impact assessments;
d) Recommend capacity building for staff involved in data processing; and
e) Conduct and report on data privacy impact assessment on behalf of the Sacco.

2.2.4 ICT Manager

The Sacco's ICT Manager has the following duties and responsibilities under this policy;

a) Protecting the Sacco's technology resources including networks, infrastructure and systems to ensure policy objectives are always achieved; and
b) Act as the reporting office for data breaches.

2.2.5 Internal Audit Function

The Sacco's Internal Audit function is responsible for independent review and reporting on compliance to this policy and making recommendations for addressing any noted gaps. They may also be called upon to investigate any related incidences and advise the Sacco on resolution mechanisms.

2.2.6 Staff responsibilities

Staff members who process personal data about Sacco members, current and previous staff, applicants, interns, or any other individual must comply with the requirements of this policy. Staff members must ensure that:

a) All personal data is kept securely;
b) No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorized third party;
c) Personal data is kept per the Sacco's retention schedule;
d) Any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Data Protection Officer;
e) Any data protection breaches are swiftly brought to the attention of the Finance and Administration Committee for staff data and the Data Protection Officer, and that they support the team in resolving breaches;
f) All staff shall sign confidentiality agreements as part of the standard onboarding process; and
g) Where there is uncertainty around a data protection matter advice is sought from the Human Resource Manager for staff data or the Data Protection Officer.

Where members of staff are responsible for supervising external service providers doing work that involves the processing of personal information, they must ensure that such external persons are aware of the Sacco's organizational Data Protection principles.

Staff who are unsure about who are the authorized third parties to whom they can legitimately disclose personal data should seek advice from the CEO through their line managers.

2.2.7 Third-Party Data Processors

Where external companies are used to process personal data on behalf of the Sacco, responsibility for the security and appropriate use of that data remains with the Sacco. Where a third-party data processor is used:

a) A data processor must be chosen which provides enough guarantees about its security measures to protect the processing of personal data;
b) Reasonable steps must be taken by the Sacco to verify that such security measures are in place;
c) A written contract establishing what personal data will be processed and for what purpose must be set out; and
d) A data processing agreement must be signed by both parties incuding a Non Disclosure Agreement.

In the event of termination of partnership, all personal data collected for or on behalf of the Sacco by the third party shall be returned to Fundilima Sacco as stipulated in the agreement except where exceptions were provided for in the signed service level agreements (SLA's) or where there are legitimate reasons to do so such as consent of data subjects.

2.2.8 Contractors and Temporary Staff

The Sacco is responsible for the use made of personal data by anyone working on its behalf. The Sacco shall ensure that contractors and staff working on short-term engagement are appropriately vetted for the data they will be processing. In addition, managers should ensure that:

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

2.3 Data Communication

The Sacco employees, directors and service providers regularly share communications that include personal data collected from its members. Based on the sensitivity of the data being shared, the Sacco will determine appropriate channels for use in disseminating selected data and consequent information. Available channels for data communication include internal memos, Sacco intranet, Email and website among others.

2.4 Data Cleansing

Data cleansing is the process of remediating data quality issues identified while profiling data within systems. This is typically done to meet regulatory requirements, business requirements and internal needs. Some of the issues from which cleansing arises are; data duplicates, obsolete or inactive records, incorrect data and incomplete records. It is the Sacco's policy to get all the required data at first instance and update it accurately for every data subject. Despite this effort, gaps may arise from time to time and they must be remedied promptly by the relevant user department.

2.5 Data Classification

Data classification is the process of sorting and categorizing data into various types, forms or any other distinct class based on its sensitivity. The Sacco classifies its data into the following categories;

Category	Description
Highly Sensitive Data	Highly sensitive data refers to data and information that must be guarded due to proprietary, ethical, privacy or business process considerations. Distribution is limited to a few individuals performing certain roles and disclosure is strictly on a need to know basis. External disclosure must be expressly authorized by the CEO in consultation with the Board. Examples of such data include business strategy, staff health records, staff payroll information and litigation records among others. To achieve this, there will be stringent access control and users will be reviewed to confirm compliance with policy.
Confidential Data	Confidential data is information protected by government regulations, statutes, industry regulations or specific internal policies. A breach could lead to legal liability, damage to Sacco reputation or financial loss. Distribution is limited to authorized users within the Sacco and disclosure may only be made to the data subject in the normal course of business or parties with a legitimate reason to know e.g. loan guarantors upon default of the principal

	borrower. Examples of such data include supplier contracts, member information and employee records among others. To achieve this, there will be stringent access control and users will be reviewed to confirm compliance with policy.
For Internal Use Only	Data for internal use only is information whose circulation is restricted to staff and directors only. Internal memos and communication sent on staff emails are examples of information meant for internal use only.
Public Data	Public information that can be communicated without restrictions and is intended for general public use. Examples include product information, Sacco vision and mission that are openly published on the Sacco website and external communications.

Table 1: Data Categories

3.0 PERSONAL INFORMATION MANAGEMENT

3.1 JUSTIFICATION FOR COLLECTING PERSONAL INFORMATION

The Sacco may collect and use Data Subject's personal data:

a) If it is necessary for the Sacco's legitimate interest and so long as its use is fair, balanced and does not unduly impact data subject's rights;
b) With the Data Subject's consent. For example, to send marketing emails, to take and use a data subject's photograph, to collect relevant medical information. The data subject can withdraw consent for this at any time.
c) As required to fulfil the Sacco's legal obligations as a registered Deposit Taking Co-operative Society and employer. This includes sharing personal info with bodies such as SASRA, Ministry or the day responsible for co-operatives, NSSF, NHIF, Courts, Police, EACC, CRBs, among other legal/statutory bodies.

The Sacco will only process sensitive personal data if it has the data subject's explicit consent. In extreme situations, the Sacco may share data subject's personal details with the emergency services if it believes it is in the data subject's '*vital interests*' to do so.

3.2 SOURCES OF PERSONAL INFORMATION

The Sacco may collect information about a data subject from different sources, for example:

i. Directly from data subject when they:
    - Apply for membership
    - Apply for account opening
    - Apply for Sacco loan products
    - Apply for employment/internship
    - Are employed in the Sacco
    - Apply as a supplier
    - Register for or at one of the Sacco's events
    - Complete a survey

- Subscribe for updates via Sacco's mobile and electronic services

ii. Indirectly:

a) From other people who think that the data subject may be interested in collaborating in our work.

b) From the public domain when the data subject has deliberately made the data public.

c) From third parties such as previous or current employers to verify details about job applicants.

d) From external sources such as publications and external reviewers or advisors.

e) From another source when the guardian appointed has consented to the collection in cases where the data subject has an incapacity.

f) Where collection of data from another source is necessary:

- for the prevention, detection, investigation, prosecution and punishment of crime;
- for the enforcement of a law which imposes a pecuniary penalty; or
- for the protection of the interests of the data subject or another person.

3.3 Forms of Personal Information Collected

The Sacco only collect personal information that is genuinely needed for its operations. This may include:

- Contact details such as name address, email address and phone numbers
- Biometric data such as thumbprints
- Nationality
- National ID and Passport information
- Date of birth
- Gender
- Information about race and ethnicity
- Qualifications
- Bank account details

- Medical information
- Benefits received
- Employment details
- Photographs and video recordings
- Tax and residency status for statutory requirements
- References from previous employers or educational institutions
- Contact details for family members and next of kin
- Details of criminal convictions

3.4 Data Subject Consent

A data subject may before the processing of their personal data give consent either orally or in writing and may include a handwritten signature, an oral statement, or use of an electronic or other media to signify agreement. The Sacco shall seek consent from data subjects through various means. These include the data subjects willingly:

i. Appending their signature of acceptance of terms and conditions of engagement on a physical consent form.
ii. Ticking an opt-in box on paper or electronically.
iii. Clicking an opt-in button or link online.
iv. Responding to an email requesting consent.
v. Volunteering optional information for a specific purpose.
vi. Selecting from equally prominent Yes/No options.

In obtaining consent from a data subject, the Sacco shall ensure that the data subject:

a) Has the capacity to understand and communicate their consent;
b) Is informed of the nature of the processing in simple and clear language that is understandable;
c) Is informed whether data is being transferred to a third party or implementing partners, or whether data is being collected by a third party on behalf of Fundilima Sacco.

d) Is informed of their duty to keep the Sacco informed of changes to their personal data and status.
e) Is informed of the right to access to their personal data or correction or deletion of it.
f) Is informed of the procedure to lodge a complaint in case of a suspected breach.
g) Is informed of the importance of providing accurate and complete information.
h) Voluntarily gives consent and that the consent is specific.

3.5 Confidentiality of Data Processing

Personal data is subject to data secrecy. Any unauthorized collection, processing, or use of such data by employees is prohibited. Any data processing undertaken by an employee that has not been authorized to carry out as part of their legitimate duties is prohibited. The "*need to know*" principle applies. Employees may have access to personal information only as is appropriate for the type and scope of the task in question. This requires a careful breakdown and separation, as well as implementation, of roles and responsibilities.

Employees are forbidden to use personal data for private or commercial purposes, to disclose it to unauthorized persons, or to make it available in any other way. Supervisors must inform their employees at the start of the employment relationship about the obligation to protect data secrecy. The staff shall therefore sign an oath of secrecy at the time of engagement by the Sacco. This obligation shall remain in force even after employment has ended.

3.6 Data Processing Security

Personal data must be safeguarded from unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification or destruction. This applies regardless of whether data is processed electronically or in paper form. Before the introduction of new methods of data processing, particularly new ICT systems, technical and organizational measures to protect personal data must be defined and implemented. These measures must be based on the state of the art, the risks of processing, and the need to protect the data.

In particular, the responsible user departments or staff should consult with the Sacco's ICT Manager. The technical and organizational measures for protecting personal data are part of the Sacco's data security management and will be adjusted continuously to the technical developments and organizational changes.

3.7 Data Retention Policy

The Sacco will hold personal information for as long as is necessary and will therefore not retain personal information if it is no longer required. In some circumstances, the Sacco may legally be required to retain data subject's personal information, for example for finance, employment or audit purposes.

4.0 DATA PROTECTION AND PRIVACY

4.1 Data Protection Principles

In processing personal data, Fundilima Sacco shall be guided by the principles of data protection as captured in the Data Protection Act, and requires the Sacco to ensure that personal data is:

a) Processed in accordance with the right to privacy of the data subject;
b) Processed lawfully, fairly and in a transparent manner in relation to any data subject;
c) Collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
d) Adequate, relevant, limited to what is necessary for 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 Sacco the Sacco and the country, unless there is proof of adequate data protection safeguards or consent from the data subject.

In complying with the stated data protection principles, Fundilima Sacco will observe the following:

4.1.1 Fairness and lawfulness

When processing personal data, the individual rights of the data subjects must be protected. Personal data must be collected and processed legally and fairly. Processing personal data is only lawful if it fulfils at least one of the following criteria:

a) If the data subject has unambiguously given consent;
b) If processing is necessary for the performance of a contract;
c) If processing is necessary for compliance with a legal obligation to which the Sacco is a subject;
d) If processing is necessary to protect the vital interests of the data subject;
e) If processing is necessary for the performance of a task that is carried out in the public interest or in the exercise of official authority vested in the Sacco; and
f) If processing is necessary for a purpose that concerns the Sacco's legitimate interest (e.g. defaulters).

4.1.2 Restriction to a specific purpose

Personal data can be processed only for the purpose that was defined before the data was collected. Subsequent changes to the purpose are only possible to a limited extent and require substantiation.

4.1.3 Transparency

The data subject must be informed of how his/her data is being handled. In general, personal data must be collected directly from the individual concerned. When the data is collected, the data subject must either be aware of or informed of:

a) The identity of the Data Controller
b) The purpose of data processing
c) Third parties or categories of third parties to whom the data might be transmitted if any.

4.1.4 Data reduction and data economy

Before processing personal data, the Sacco will determine whether and to what extent the processing of personal data is necessary to achieve the purpose for which it is undertaken. Where the purpose allows and where the expense involved is in proportion with the goal being pursued, anonymized or statistical data must be used. Personal data may not be

collected in advance and stored for potential future purposes unless required or permitted by national law.

4.1.5 Deletion

Personal data that is no longer needed after the expiration of legal or business process-related periods must be deleted. There may be an indication of interests that merit protection or historical significance of this data in individual cases. If so, the data must remain on file until the interests that merit protection have been clarified legally, or the Sacco has evaluated the data to determine whether it must be retained for historical purposes.

4.1.6 Factual accuracy; up-to-date data

Personal data on file must be correct, complete, and – if necessary – kept up to date. Suitable steps must be taken to ensure that inaccurate or incomplete data are deleted, corrected, supplemented or updated.

4.1.7 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 organizational and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification or destruction.

4.2 Rights of Data Subjects

Every data subject has the following rights:

a) To be informed of the use to which their personal data is to be put;
b) To access their personal data in the custody of the Sacco;
c) To object to the processing of all or part of their personal data. This does not apply if a legal provision requires the data to be processed;

d) To the correction of false or misleading data; and
e) To deletion of false or misleading data about them.

A right conferred on a data subject may be exercised:

a) By a person who has parental authority or by a guardian if the data subject is a minor;
b) By a person duly authorized to act as a guardian or administrator in a case where the data subject has a mental or other disability; or
c) By a person duly authorized by the data subject.

4.3 Necessity in Data Processing

Some of the processing operations are driven by necessity and may not require explicit consent like CCTV surveillance & recording, telephone recordings and staff Email monitoring. In this case, individual consent or opting out is not practical, so Fundilima Sacco will issue prominently displayed or explained notifications to users that their data may be collected if they access certain locations or services.

4.4 Direct and Electronic Marketing

The Sacco may send periodic promotional messages and to members and prospective members using its various platforms like email and SMS among others. These require the explicit consent of the subject and clear instructions for opting out must be provided to the member. A member's decision to opt-out of such communications must be respected and observed until revoked voluntarily and explicitly. This policy notwithstanding, the Sacco may send promotional material in response to a member request and add them to a mailing list for future similar correspondence until the member opts out.

5.0 DATA BREACH RESPONSE PLAN

A data breach refers to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Personal data is any information relating to an identified or identifiable person including reference to their name, identification number or other factors relating to their identity. It is the responsibility of any employee who notices a breach to escalate to the Data Protection Officer through their immediate supervisor for incident recording and resolution. Once reported, the DPO shall conduct a preliminary inquiry into the matter and advise the CEO on an appropriate response plan based on preliminary findings. In general, a response plan may involve;

a) Containment measures to limit the impact of the breach;
b) Evaluation of the breach to inform any administrative action and future prevention;
c) Notification to all affected parties recommending any necessary actions to safeguard their data e.g. changing access passwords; and
d) Implementation of mechanisms to prevent future recurrence e.g. policy review.

6.0 AUTOMATED DECISION MAKING

To deliver its products and services efficiently, the Sacco may automate some aspects of decision making to meet member requests. This includes but is not limited to determining eligibility for loans and respective loan limits. Where decisions are automated, the Sacco must inform members that their requests will be processed and determined by automated systems. The member has a right to appeal for review of any such decisions.

7.0 INFORMATION SHARING

Fundilima Sacco keeps all personal data collected during its business confidential. The Sacco may however share this data with its service providers to the extent required to deliver its services and ensure business continuity. Such service providers include contracted transaction processing platforms e.g. mobile banking and data backup service providers,

Credit Reference Bureaus, debt recovery agencies and government agencies like Kenya Revenue Authority and law enforcement agencies among others. In all such instances, the Sacco will ensure the agreements signed and attendant data processing operations are conducted in strict adherence to the Data Protection Act.

8.0 CAPACITY BUILDING

All Sacco officials and staff are expected to familiarise themselves with the content of this Policy. To enhance compliance with this Policy, the Sacco shall organize periodic sensitization forums for Sacco officials and staff members.

9.0 COMPLIANCE

9.1 All officials, staff and stakeholders of the Sacco shall comply with the provisions of this Policy. Non-compliance shall constitute misconduct.

9.2 To ensure compliance, officials, staff of the Sacco shall sign an oath of confidentiality committing to treat accessed personal information securely and in confidentiality. Stakeholders' contracts shall have a clause on confidentiality on accessed personal information. The oath shall be binding during and after exit from service of the Sacco.

9.3 Staff not complying with this Policy shall face disciplinary action in line with the Human Resource Policy.

9.4 Sacco officials not complying shall face disciplinary action in line with the Sacco Bylaws, Board Charter and relevant laws and regulations.

9.5 External service providers not complying with the provisions of this policy will be handled following provisions of contracts signed.

POLICY REVISION

This Policy shall be reviewed periodically and may be amended as conditions warrant. Amendments to this Policy may be recommended by staff through the manager or by individual Directors as necessary and submitted to the Board, provided the changes in no way affect the substance or intent of this Policy. Amendments and updates to this policy shall become effective only when adopted by a BOD resolution.

ADOPTION OF POLICY

This document may be cited as the Data Protection Policy for Fundilima Sacco Society Limited and has been discussed and adopted for implementation this …….. day of …….. 2022.

SIGNED FOR AND ON BEHALF OF FUNDILIMA SACCO SOCIETY LIMITED:

1. Name: _____ Designation: **Chairman**

Sign: _____ Date: _____

2. Name: _____ Designation: **Honorary Secretary**

Sign: _____ Date: _____

3. Name: _____ Designation: **Treasurer**

Sign: _____ Date: _____

4. Name: _____ Designation: **Chief Executive Officer**

Sign: _____ Date: _____

APPENDICES

Appendix 1: OATH OF SECRECY/ CONFIDENTIALITY

I, the undersigned, _____,

(FULL NAMES)

National ID Number:_____ and PF Number: _____

being an employee of Fundilima Sacco Society Ltd, hereby declare:

That I will treat securely and observe strict confidentiality in respect to all personal data relating to Sacco officials, staff, members/customers and stakeholders and will not reveal any of the matters which may come to my knowledge in the discharge of my duties during and after engagement by the Sacco, except where and when required to do so by the Board of Directors, the Supervisory Committee, The CEO, or other person duly authorized in writing by the Society or by a court of law, or by any other person to whom such matters relate provided such person is entitled to be informed in respect thereof.

Signature: _____ Role: _____

Date: _____

Witnessed by:

_____

(FULL NAMES)

Signature of Witness: _____ Date _____

Appendix 2: THIRD PARTIES/ PARTNER NON-DISCLOSURE AGREEMENT

We/I, the undersigned, _____,

(FULL NAMES)

being service provider(s) of Fundilima Sacco Society Ltd, hereby declare that:

We/I undertake that during the operation of, and after the expiration, termination or cancellation of this appointment, for any reason, we/I will keep confidential any proprietary or confidential data/information relating to the Sacco or its services or members/customers or stakeholders.

Any studies, reports or other materials, graphics, software or otherwise received or prepared by us/me from/for the Sacco under this Agreement shall belong to and remain the property of the Sacco. We/I shall not use such property for any other purpose unless prior express consent is given by the Sacco.

Authorised signatory:

Name: _____ Designation: _____

Signature: _____ Date: _____

Witnessed by:

Name: _____ Signature: _____

Date: _____