DATA PROTECTION POLICY

POLICY	DATA PROTECTION POLICY
AUTHOR (S)	HEAD, COLLECTIONS AND DATA ANALYTICS (DATA PROTECTION SUPERVISOR) HEAD, INFORMATION COMMUNICATION TECHNOLOGY
OWNER	HEAD, COLLECTIONS AND DATA ANALYTICS (DATA PROTECTION SUPERVISOR)
RECIPIENTS	EXECUTIVE MANAGEMENT HEADS OF DEPARTMENT RISK MANAGEMENT AND COMPLIANCE INTERNAL AUDIT ALL STAFF
VERSION	2.1

Connected procedures/policy
Description
The Data Protection Act, 2012 (Act 843)
Information Security Compliance Policy
Cybersecurity Policy
Acceptable Use Policy
Information Security Breach and Incidence Response Policy
Record Retention Policy

Objectives

The Policy aims to achieve the following objectives for the Company:

a. Ensure compliance with data protection legislation and adherence to best practices.
b. Safeguard the rights of stakeholders and other involved parties, including but not limited to staff, clients, and partners.
c. Mitigate the risk of data breaches and security threats, including:
    i. Unauthorized disclosures of confidential information.
    ii. Potential reputational harm resulting from successful hacking attempts to access sensitive data.

CONTENTS

1.0 INTRODUCTION

The Data Protection Policy (referred to as "the Policy") of StarLife Assurance Limited Company (referred to as "the Company") is dedicated to ensuring responsible handling of personal data. It delineates the legal obligations governing the collection, storage, destruction, transfer and disclosure of personal data.

The Company requires processing certain personal data of various data subjects to facilitate its operational functions. These data subjects encompass staff concerning their employment contracts, clients in connection with business relations, office visitors, contractors/third-party suppliers, directors, shareholders, and other individuals with whom the Company maintains a relationship or may need to communicate.

The policy adopted by the Company is in Compliance with the Data Protection Act, 2012 (Act 843).

The information obtained from these data subjects is protected by law and the Company is obliged to ensure compliance. To this end, the Company is committed to:

a. Restricting and monitoring access to sensitive data;
b. Developing transparent data collection procedures;
c. Training staff in online privacy and security measures;
d. Building secure networks to protect online data from cyber-attacks;
e. Establishing clear procedures for reporting privacy breaches or data misuse;
f. Including contract clauses and communicating statements on how the Company handles data;
g. Protecting the rights and privacy of individuals;
h. Establishing data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.); and,
i. Communicating its data protection provisions on its website.

2.0 DEFINITIONS

For the purpose of the policy, the following definitions apply:

a. **"The Company"** refers to StarLife Assurance Limited Company;
b. **"The Policy"** refers to the Data Protection Policy;
c. **"The Act"** refers to the Data Protection Act, 2012 (Act 843);
d. **"Data Protection"** means the process of safeguarding information from loss, corruption or compromise;
e. **"Personal Data"** is any information that can enable an individual to be identified;
f. **"Special Category Data"** is sensitive information that relates to race, ethnic origin, political opinions, religious or philosophical beliefs, biometric data etc.;

g. **"Processing Data"** means obtaining, recording, holding or adding to the information or data or performing any operation on the information or data;
h. **"Data Controller'** means the person or organization who determines the purpose of the data i.e. how the data should be processed or used;
i. **"Data Subject"** means an individual whose personal data is being processed;
j. **"Data processor"** means any person or organization who processes the data;
k. **"Consent"** means giving permission for something to happen or an agreement to do something;
l. "**Electronic Data**" means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically;
m. **"Privacy Notices"** is a statement that discloses some or all of the ways a party gathers, uses, discloses and manages a customer or client data;
n. "Staff" refers to employees and agents of the Company;
o. **"Right to Erasure"** is a right given to individuals to be able to request their personal data to be erased; and,
p. **"Data Breach"** is a security incident where information is accessed without authorization.

3.0 PURPOSE

The policy aims to achieve the following but not limited to:

a. Complying with the Data Protection Act 2012 (Act 843);
b. Ensuring that data collected are processed in accordance with the Act;
c. Providing guidance on the standards of conduct and practice that must be complied with;
d. Protecting the rights of data subjects;
e. Protecting the Company from the risk of data breach and data security risks, including:
    i. Unauthorized disclosures of confidential information; and,
    ii. Potential reputational harm resulting from successful hacking attempts to access sensitive data.

4.0 APPLICATION AND SCOPE

The policy applies to all staff of the Company.

The encompasses all Company information, regardless of its format (whether oral, written, pictorial, or electronic media), including but not limited to materials of technical, operational, administrative, economic, planning, business, financial, or legal nature, as well as any intellectual property.

The policy covers the following:

a. Collection and processing of personal data;
b. Data protection principles;
c. Roles and responsibilities;
d. Data storage and security;
e. Records retention;
f. Ensuring data accuracy;
g. Procedures for disclosure;
h. Processing personal data for direct marketing;
i. Requirements for registration as data controller;
j. Protocols for handling data breach;
k. Procedures for disposal of computer hardware; and,
l. Training requirements.

5.0 COLLECTION OF PERSONAL DATA

The Company receives personal data in any format (written or oral) from data subjects
or other information in the possession of, or likely to come into the possession of the Company.

Personal data can be factual such as the following but not limited to:

a. Names of individuals;
b. Postal addresses;
c. Email addresses;
d. Telephone numbers;
e. Date of birth;
f. Images or photographs or any genetic information; and,
g. Biometric data used for identification purposes;
h. Any other personal information relating to individuals

Typically, the Company will obtain personal data directly from the data subject. However, in certain circumstances, the Company may collect personal data indirectly when:

a. The data is contained in a public record;
b. The data subject has deliberately made the data public;
c. The data subject has consented to the collection of the information from another source;
d. The collection of the data from another source is not likely to prejudice a legitimate interest of the data subject;
e. The collection of the data from another source is necessary:
   for the prevention, detection, investigation, prosecution or punishment of an offence or breach of law;
   i. For the enforcement of a law which imposes a pecuniary penalty;
   ii. For the enforcement of a law which concerns revenue collection;
   iii. For the conduct of proceedings before any court or tribunal that have commenced or are reasonably contemplated;
   iv. For the protection of national security; or
   v. For the protection of the interests of a responsible or third party to

whom the information is supplied;

f. Compliance would prejudice a lawful purpose for the collection; or
g. Compliance is not reasonably practicable

5.1 Special data

Special data includes special categories data that are particularly sensitive and therefore warrants additional protection. The Company shall not process special personal data unless such processing is deemed necessary and the consent of the data subject has been obtained.

Special personal data consists of information about an individual that relates to:

i. The race, colour, ethnic or tribal origin;
ii. The political opinion;
iii. The religious beliefs or other beliefs of a similar nature;
iv. The physical, medical, mental health or mental condition or deoxyribonucleic acid (DNA);
v. Sexual orientation;
vi. Trade union membership;
vii. Commission or alleged commission of an offence; or
viii. Proceedings for an offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in the proceedings

6.0 DATA PROTECTION PRINCIPLES

The Act establishes principles governing the processing of personal data, mandating that personal information be collected and utilized fairly, stored securely, and not unlawfully disclosed. These regulations are applicable regardless of whether the data is stored electronically, on paper, or on other mediums. In processing data, the Company shall prioritize the privacy of the data subject by adhering to the following principles:

a. Accountability: The Company shall ensure that Personal Data is processed:
    i. Without violating the privacy rights of the data subject;
    ii. In accordance with legal requirements; and
    iii. In a that is reasonable manner.

    In cases where the data pertains to foreign data subjects and is sent to Ghana for processing, will ensure compliance with the data protection legislation of the data subject's country. The Company will refrain from transferring data to organizations or countries lacking adequate data protection regulations.

b. Lawfulness of processing: Personal data must be processed only if the purpose for which it is processed is necessary, relevant and not excessive. The Company shall not process personal data without the prior consent of the data subject unless the processing is:

i. Necessary for the purpose of the employment, insurance or other contract to which the data subject is a party;
ii. Authorized or required by law;
iii. To protect a legitimate interest of the data subject;
iv. Necessary for the proper performance of a statutory duty; or
v. Necessary to pursue the legitimate interest of the Company or a third party to whom the data is supplied.

Furthermore, the Company will not retain personal data beyond the necessary duration required to fulfill the purpose for which it was collected and processed.

Personal data will only be processed by a third party upon prior written authorization from the Company. The third party will be obligated to treat the data with confidentiality. Accordingly, the Company will ensure that non-disclosure agreements are executed or that specific confidentiality/data protection clauses are included in contracts where third parties will be provided with data.

c. Specification of purpose: The Company shall collect data for specific, explicitly defined, lawful purposes related to its business activities. Therefore, the data subject must always be informed of the purpose for which the data is collected.

d. Further Processing Compatibility: The Company shall ensure that any subsequent processing of personal data aligns with the original specific purpose for which it was obtained.

e. Information Quality: The Company shall ensure at all times that data is accurate, complete, up-to-date and not misleading having regard to the purpose of collection or processing.

f. Openness: The Company shall ensure that the data subject is at all times informed of:
i. The nature of the data being collected;
ii. The name and address of the Company;
iii. The purpose for which the data is required;
iv. Whether or not the supply of the data by the data subject is discretionary or mandatory;
v. The consequences of failure to provide the data;
vi. The authorized requirement for the collection of the information or the requirement by law for its collection;
vii. The recipients of the data, if any;
viii. The nature or category of the data; and,
ix. The existence of the right of access to and the right to request rectification of the data collected before the collection.

Where data is obtained from a third party, the Company shall ensure the data subject is given the information specified above before or as soon as practicable after the collection of the data.

g. Data security measures: The Company shall take necessary steps to secure the integrity of personal data in its possession or control through the adoption of appropriate, reasonable, technical and organizational measures to prevent loss of, damage to or unauthorized destruction; an unlawful access to or unauthorized processing of personal data.

   In cases where the Company engages a third party to process personal data, the Company shall ensure that the third party establishes and complies with the data protection requirements in the policy and under law.

   In instances where the Company has reasonable grounds to suspect that the personal data has been accessed or acquired by an unauthorized person, the Company shall notify the Data Protection Commission and the data subject as soon as reasonably practicable. The Company shall then take steps to restore the integrity of the information system.

h. Data subject participation: The Company shall upon request by the data subject and upon proof of identity;
   i. Confirm whether or not it holds personal data about that data subject;
   ii. Provide details of the personal data it holds, including data about the identity of any third party who has or has had access to the information;
   iii. Correct data held on the data subject; and
   iv. Modify, erase, reduce or correct data in its custody.

   The Company is mandated to notify the data subject of the action taken as a result of the request.

i. Rights of the individual: The rights of all individuals should be respected when processing personal data. These are enshrined in the legislation as follows:
   i. The right to be informed;
   ii. The right of access;
   iii. The right to rectification;
   iv. The right to erasure;
   v. The right to restrict processing;
   vi. The right to data portability; and,
   vii. The right to object.

   The rights above depend upon the lawful basis for processing. For example, the right to erasure only applies where the lawful basis for processing is consent. Where other basis for processing are used such as public task, legitimate interests, contractual basis or legal requirement are used, the right of rectification, restriction and the right to object are also limited to ensuring that the data is accurate before it can be processed.

   However, the right to be informed is considered fundamental and

applies universally in all situations.

j. Data protection by default:
Where the company is undertaking new processing (e.g. it is collecting a new type of data or it is implementing a new system or process) it must consider building in data protection from the outset, including the organizational and technical measures to ensure appropriate security.

New processing must be approved before collection is started and signed off by the Data Protection Supervisor.

k. Data Minimization:
In accordance with the Act, the Company is obligated to ensure that it collects only necessary data. Individuals responsible for data collection should, therefore, ensure that it is limited to what is required. Staff are required to evaluate whether any data being collected is necessary for the intended purpose. Where processing can take place without this data it should not be collected.

l. Transparency:
The Company is required to provide specific information to individuals regarding the processing of their personal data. This information needs to be actively provided to individuals in a way that is:

i. Concise;
ii. Transparent;
iii. Intelligible;
iv. Easily accessible; and
v. Clear.

To provide this information the Company must provide a privacy statement which is published on the website and made available to all clients. The privacy Statement must include the following:

i. The name of company and contact details;
ii. The contact details of the data protection officer;
iii. The purposes of the processing;
iv. The lawful basis for the processing;
v. The categories of personal data obtained;
vi. The recipients or categories of recipients of the personal data;
vii. The retention periods for the personal data;
viii. The rights available to individuals in respect of the processing;
ix. The right to withdraw consent;
x. The right to lodge a complaint;
xi. The source of the personal data; and,
xii. The details of whether individuals are under a statutory or contractual obligation to provide the personal data.

Staff may only process data for the specific purposes communicated to the data subject at the time of initial data collection or for any other purposes specifically permitted by the Legislation. Personal data must

not be collected for one purpose and then used for another purpose without informing the data subject of the new purpose before any processing occurs. The only exception to this is the use of research data.

6.1 Exception

Personal data is exempt from the data protection principles if it consists of confidential references provided by the Company for the purposes of:

a. Education, training or employment of data subject;
b. The appointment to an office of the data subject;
c. The provision of any service by the data subject; and,
d. Disclosure by the law enforcement agencies.

7.0 ROLES AND RESPONSIBILITIES

Staff and all third parties who deal with the Company have some responsibility for ensuring that data is collected, stored and handled appropriately and must therefore ensure that data is handled and processed in accordance with the policy. However, the following persons have key areas of responsibility:

a. Board of Directors: shall be ultimately responsible for ensuring that the Company meets its legal obligations as it pertains to data protection are met.

b. Executive Management: shall nominate the Head, Collections and Data Analytics or such other staff of the Collections and Data Analytics Department as the Data Protection Supervisor (DPS) and shall provide the necessary training and facilities to ensure that the person appointed is qualified for certification as the Data Protection Supervisor in accordance with the criteria established by the Data Protection Commission.

c. Data Protection Supervisor shall be responsible for:
    i. Monitoring the Company's compliance with the Act;
    ii. Keeping the Board of Directors updated about data protection responsibilities, risks and issues;
    iii. Reviewing all data protection procedures and related issues;
    iv. Arranging data protection training for staff and other stakeholders;
    v. Addressing data protection concerns from data subjects such as staff and clients;
    vi. Dealing with requests from individuals to inspect the data the Company holds about them; and
    vii. Actively participating in reviewing and approving contracts or agreements with third parties that may handle the Company's sensitive data.
    viii. To be the first point of contact for supervisory authorities; and,
    ix. To advise on, and to monitor, data protection impact assessments.

d. Head, ICT shall be responsible for:
    i. Ensuring all systems, services and equipment used for storing

data meet acceptable security standards;
ii. Performing regular checks and scans to ensure security hardware and software is functioning properly;
iii. Implementing appropriate remedial measures to restore the integrity of data which is lost, corrupted or compromised; and
iv. Evaluating any third party services which the Company intends to use for data storage or processing.

e. Head, Brand & Communication shall be responsible for:
   i. Approving any data protection statements attached to communications such as emails, advertisements, publications and letters;
   ii. Addressing any data protection queries from journalists or media outlets upon the prior approval of the Executive Management; and,
   iii. Where necessary working with other staff to ensure marketing initiatives comply with data protection principles;

f. All staff, shall be responsible for:
   i. Ensuring that they understand their obligations outlined in the policy and understands how to safeguard personal data. They are required to adhere to the provided guidance at all times; and,
   ii. Reporting any breach or potential incident, likely to result in unauthorized disclosure, damage, destruction or loss of personal data directly to the Data Protection Supervisor.

7.1 General Responsibilities
The Company shall;

i. Limit access to data covered by the policy to individuals strictly on a "need-to-know" basis to facilitate their job responsibilities;
ii. Provide comprehensive training to all staff to help them understand their responsibilities when handling data;
iii. Ensure staff keep all data secure, by taking necessary precautions and adhering the guidelines outlined in the policy and such other guidelines pertaining to data handling that may be issued from time to time;
iv. Implement strong and encrypted passwords policy to secure data.
v. Prohibit the unauthorized disclosure of personal data individuals both within and outside the Company;
vi. Regularly review and update personal data, deleting and disposing of any data that is outdated or no longer necessary; and,
vii. Implement a data access request process for obtaining access to confidential information; staff, clients and other third parties shall submit requests from the appropriate authority in writing.

The staff shall;

i. Seek assistance from the Head, ICT or Head, CDA if they are unsure about any aspect of data protection;
ii. Never share Passwords with others;
iii. Refrain from sharing data informally; when access to confidential

information is required, request from the appropriate authority in writing; and,

iv. Comply with the policy.

8.0 DATA STORAGE AND SECURITY

These rules describe how and where data should be safely stored and the necessary security measures in place to protect data. It is the responsibility of the relevant HoDs to ensure that centralized records are stored, maintained and secured to meet the needs and reasonable expectations of staff and other stakeholders.

8.1 Data Storage

The Company stores data in the following format:

a. Paper;
b. Electronic;
c. Digital; and,
d. Cloud.

8.1.1 Data Stored on Paper

When data is stored on paper, it must be stored in a secure place where unauthorized persons cannot access. Among others:

a. When not required, the paper or files should be kept in a locked drawer or filing cabinet.
b. Staff must ensure paper and print outs are not left where unauthorized persons can see them, for instance on a printer; and,
c. Data print outs should be shredded and disposed of securely when no longer required.

These guidelines also apply to electronically stored data that has been printed.

The record retention policy shall be complied with.

8.1.2 Electronically Stored Data

Electronically stored data it shall be protected from unauthorized access, accidental deletion and malicious hacking attempts. The following shall apply:

a. Data shall be protected by strong passwords that are changed regularly and never shared between staff;
b. If data is stored on removable media (like CD, DVD, External Drive, etc.), these shall be kept locked away securely when not in use;
c. Data shall only be stored on designated drives and servers, and shall only be uploaded to approve cloud computing services;
d. Servers containing personal data shall be sited in a secure location away from the general office space;
e. Data shall be backed up frequently and tested regularly, in line with the Company's standard backup procedures;
f. Data shall not be saved directly to mobile devices such as tablets or smartphones;

g. All servers and computers containing data shall be protected by approved security software and firewalls;
h. Computer screens of staff shall always be locked when unattended; and,
i. Data shall be encrypted before being transferred electronically outside the Company.

8.1.3 Digital and Online Stored Data

Digital and online stored data shall have the necessary storage systems to protect it from unauthorized access, accidental deletion and malicious hacking attempts. The following shall apply:

a. Data shall be protected by strong passwords that are changed regularly and never shared between staff.

8.1.4 Data Storage on Cloud

The Company primarily stores data on cloud-based platforms such as Amazon Web Services, eliminating the need for physical data centers. The Company will ensure data stored in the cloud is automatically protected and secured against unauthorized access, accidental deletion, and malicious hacking.

8.2 Data Security

The Act requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorized or unlawful processing and against accidental loss, destruction or damage. It requires that the Company put appropriate measures in place to secure the data. The ICT department is responsible for working with data owners to ensure appropriate security measures are in place.

All staff are responsible for ensuring personal data are kept securely and accessible only to those who need to use it. Appropriate security measures are to be taken to prevent accidental loss of, or damage to personal data. This will mean the use of passwords or encryption for electronic documents and keeping paper records under lock and key.

The transport of personal data in any format (laptop, hard copy, memory stick etc.) should be avoided whenever possible. This applies especially to special categories data, large volumes of personal data, or information which could cause particular harm or distress if lost. Only in exceptional circumstances should this information be transported outside of the office premises. staff who do so should always ensure that it is kept with them at all times.

The Company shall ensure that all mobile devices (laptops, smartphones, tablets) and external storage media (USB sticks, external hard drives, DVDs, CDs, etc.) used to transport personal data and special categories data outside the Company are secured by deploying strong encryption.

Any loss/theft must be immediately reported to the Data Protection Supervisor and the Head, ICT as this represents a breach of the policy and must be recorded and reviewed for any action required.

9.0 RECORDS RETENTION

The Company's records shall be maintained by the ICT Department.

The records retention policy outlines the duration for retaining various types of documents. Staff should regularly review their records to ensure that the documents they hold are destroyed within the relevant destruction time limit in accordance with the records retention schedule. Where the documentation contains personal information, the destruction must take place confidentially (e.g. shredding, disposal as confidential waste, secure electronic deletion).

10.0 DATA ACCURACY

The Act requires the Company to maintain accurate and up-to-date data. The Company shall therefore establish appropriate measures to ensure that data is accurate at all times. It is the responsibility of all staff to take reasonable steps to ensure that data is kept as accurate and up-to-date as possible.

Data should be stored in the minimum number of locations necessary. Staff shall not create any unnecessary additional data sets. Additionally, staff shall ensure at every opportunity that data is updated, such as by confirming a client's details when they call or visit the office.

The Company shall facilitate data subjects in updating their information held by the Company. Data shall be promptly updated upon discovery of inaccuracies.

11.0 DISCLOSURE

The Company shall disclose personal data to law enforcement agencies without the consent of the data subject upon satisfaction that the request is legitimate and upon prior approval of Executive Management and/ or the Board, if necessary.

Staff must not disclose personal data to a third party except in limited cases where there is a legal or statutory duty to do so or where consent is given. All staff must therefore take care to ensure that personal data is not disclosed to unauthorized third parties which includes family members of the data subject, friends, government bodies and the police in certain circumstances without the data subject's consent.

12.0 PROCESSING PERSONAL DATA FOR DIRECT MARKETING

The Company shall not provide, use, obtain, procure or provide information related to a data subjects for the purposes of direct marketing without the prior written consent of the data subject. Direct marketing includes communication by whatever means of advertising or marketing material which is directed to particular individuals.

The Company shall comply with all written notices from a data subject precluding the Company from processing his/her personal data for the purposes of direct marketing.

13.0 REGISTRATION AS DATA CONTROLLER

The Company is required to register and maintain its registration with the Data Protection Commission as a data controller.

14.0 BREACH

Any breaches of data protection should be reported to the Data Protection Supervisor and the Head, ICT. It is essential that staff report a breach or potential breach immediately. This allows swift action to be taken to address the breach, as well as allowing the Company to comply with its obligation to report breaches.

In cases where there is clear negligence or intent on the part of staff regarding a breach of the policy, the Company will assess the circumstances to determine appropriate actions. Disciplinary measures, in accordance with the Company's policies, may be taken against negligent staff. All relevant factors will be considered when determining appropriate actions, including the promptness of reporting the breach.

15.0 DISPOSAL OF COMPUTER HARDWARE

The ICT department have to assess computer equipment on an annual basis and advise management on the need to dispose of them primarily because:

a. Non-functionality with no feasible repair options;
b. Inability to fulfill operational requirements; and,
c. Surplus due to replacement policies or strategies.

Methods of disposal

1. Where the computer is in working order but inadequate for the designated purpose, it is expected that as far as is practicable the first consideration will be for internal re- assignment.
2. Thus it will be assigned to other departmental functions for which the capacity is appropriate.
3. Reasonable effort must be made to ascertain if there is any other department that may wish to make use of the equipment.
4. Equipment with residual value but which are inadequate for the business of the Company may be sold to staff or outside bodies, subject to the Company's financial guidelines.
5. Where equipment has little resale value, consideration should be given to donating it to a charitable endeavor.
6. If the equipment cannot be used, it should be scrapped for parts or disposed of in accordance with the Company's policy and procedures for disposal.
7. All movement of equipment must be recorded in the Asset Register, which indicates the information to be recorded over the disposal process.

8. All disposals and movement of ICT equipment shall be authorized by Head, ICT or as per delegated authority.
9. Information stored in the ICT equipment should be analyzed before approval given for deletion/disposal/re-assignment. This shall be done in consultation with the relevant stakeholders before any disposal is done

16.0 TRAINING

The following shall apply for training:

a. All staff will receive training on the policy which is mandatory as per the Act;
b. New staff will receive training as part of the onboarding process;
c. Refresher training shall be given to all staff annually or whenever there is a substantial change to the policy; and,
d. Training may be provided through in-house/online workshops or e-learning platforms.

17.0 CONSEQUENCES OF NON-COMPLIANCE

The principles contained in the policy shall be strictly complied with. Any breach of the policy shall result in the following:

a. In the case of a staff or director, disciplinary action resulting in termination of employment or appointment and or legal action for damages; and,
b. In any other case, termination of contract, legal action for breach of contract, if any and damages and regulatory redress where the third party is registered with the Data Protection Commission

18.0 REVIEW

The policy shall be reviewed annually and/or whenever necessary to ensure it is current and relevant. The policy shall also be reviewed when there are changes in regulations that will warrant policy adjustments.

19.0 DOCUMENT HISTORY

Document Name	Data Protection Policy	Date
Version	2.0	
Prepared by	Name: Legal and compliance, Data processing and analytics	
Reviewed by	Name: Executive management	
Approved by	Name: Board ICT &innovation committee	
Approved by	Name: Board of Directors	30th September 2020

Document Name	Data Protection Policy	Date
Version	2.1	
Prepared by	Name: Head, Collections and Data Analytics (Data Protection Supervisor) Name: Head, ICT	16th February 2024
Reviewed by	Name: Head, Legal Name: Head, Risk Management and Compliance	20th February 2024
Approved by	Name: Executive Committee	23rd February 2024
Approved by	Name: Board Finance, ICT and Strategy Committee	11th September 2024
Approved by	Name: Board	4th December 2024
Description of change	The following sections revised: 1. Objectives 2. Sections 1-18 revised and new sections included.	