Data Protection and Information Sharing Policy Statement and Manual of

1. INTRODUCTION

This Data Protection and Information Sharing Policy ("Policy) describes the way that **KENSINGTON HOME FOR THE AGED**, ("**KENSINGTON HOME FOR THE AGED**"), will meet its legal obligations and requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the Protection of Personal Information Act, No 4 of 2013 (POPI), as that is the key piece of legislation covering security and confidentiality of personal information. POPI requires **KENSINGTON HOME FOR THE AGED** to inform their clients/donors/beneficiaries as to the manner in which their personal information is used, disclosed and destroyed. **KENSINGTON HOME FOR THE AGED** guarantees its commitment to protecting its clients/donors/beneficiaries' privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

2. DEFINITIONS

2.1 Personal Information

Personal information is any information that can be used to reveal a person's identity. Personal information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person (such as a company), including, but not limited to information concerning:

- race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person;
- information relating to the education or the medical, financial, criminal or employment history of the person;
- any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- the biometric information of the person;
- the personal opinions, views or preferences of the person;
- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about the person;
- the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

2.2 Data Subject

This refers to the natural or juristic person to whom personal information relates, such as an individual customers/clients/residents/visitor/beneficiaries/donors or a company that supplies the organisation with products or other goods.

2.3 Responsible Party

The responsible party is the entity that needs the personal information for a particular reason and determines the purpose of and means for processing the personal information. In this case, the organisation is the responsible party.

2.4 Operator

An operator means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. For example, a third-party service provider that has contracted with the organisation to shred documents containing personal information. When dealing with an operator, it is considered good practice for a responsible party to include an indemnity clause.

2.5 Information Officer

The Information Officer is responsible for ensuring the organisation's compliance with POPIA.

Where no Information Officer is appointed, the head of the organisation will be responsible for performing the Information Officer's duties.

Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.

2.6 Processing

The act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning personal information and includes:

- the collection, receipt, recording, organizing, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- dissemination by means of transmission, distribution or making available in any other form; or
- merging, linking, as well as any restriction, degradation, erasure or destruction of information.

2.7 Record

Means any recorded information, regardless of form or medium, including:

- Writing on any material;
- Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
- Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
- Book, map, plan, graph or drawing;
- Photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced.

2.8 Filing System

Means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

2.9 Unique Identifier

Means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

2.10 De-Identify

This means to delete any information that identifies a data subject or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the data subject.

2.11 Re-Identify

In relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

2.12 Consent

Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

2.13 Direct Marketing and Fundraising

Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:

- Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or
- Requesting the data subject to make a donation of any kind for any reason.

2.14 Biometrics

Means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

3. SCOPE OF THE POLICY

This purpose of this policy is to protect the organisation from the compliance risks associated with the protection of personal information which includes:

- Breaches of confidentiality. For instance, the organization could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.
- Failing to offer choice. For instance, all data subjects should be free to choose how and for what purpose the organization uses information relating to them.

- Reputational damage. For instance, the organization could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by the organization.

This policy demonstrates the organisation's commitment to protecting the privacy rights of data subjects in the following manner:

- Through stating desired behavior and directing compliance with the provisions of POPIA and best practice.
- By cultivating an organizational culture that recognizes privacy as a valuable human right.
- By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.
- By creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of the organization.
- By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information Officers in order to protect the interests of the organization and data subjects.
- By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

4. POLICY STATEMENT

KENSINGTON HOME FOR THE AGED collects and uses Personal Information of the individuals and corporate entities with whom it works in order to operate and carry out its business effectively. **KENSINGTON HOME FOR THE AGED** regards the lawful and appropriate processing of all Personal Information as crucial to successful service delivery and essential to maintaining confidence between **KENSINGTON HOME FOR THE AGED** and those individuals and entities who deal it. **KENSINGTON HOME FOR THE AGED** therefore fully endorses and adheres to the principles of the Protection of Personal Information Act ("POPI").

The Policy applies to all employees, directors, sub-contractors, agents, and appointees. The provisions of the Policy are applicable to both on and off-site processing of personal information.

INFORMATION OFFICER(S)

The Information Officer appointed to **KENSINGTON HOME FOR THE AGED** is

Leon Courie

_____

He/She may be contacted at:

E-mail: Lcourie@mweb.co.za

Telephone number: +27 021 593 2274/85

DEPUTY INFORMATION OFFICER(S)

The Deputy Information Officer appointed to **KENSINGTON HOME FOR THE AGED** is

Marianna Maasdorp

_____

He/She may be contacted at:

E-mail: info@kenshome.co.za

Telephone number: +27 021 593 2274/85

SPECIFIC DUTIES AND RESPONSIBILITIES

4.1 Governing Body

The organisation's governing body cannot delegate its accountability and is ultimately answerable for ensuring that the organisation meets its legal obligations in terms of POPIA.
The governing body may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

The governing body is responsible for ensuring that:

- The organization appoints an Information Officer, and where necessary, a Deputy Information Officer.
- All persons responsible for the processing of personal information on behalf of the organization:
- are appropriately trained and supervised to do so,
- understand that they are contractually obligated to protect the personal information they come into contact with, and
- are aware that a willful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.
- Data subjects who want to make enquires about their personal information are made aware of the procedure that needs to be followed should they wish to do so.
- The scheduling of a periodic POPI Review in order to accurately assess and review the ways in which the organization collects, holds, uses, shares, discloses, destroys and processes personal information.

4.2 Information Officer

The organisation's Information Officer is responsible for:

- Taking steps to ensure the organizations' reasonable compliance with the provision of POPIA.
- Keeping the governing body updated about the organization's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations pursuant to POPIA.
- Continually analyzing privacy regulations and aligning them with the organizations' personal information processing procedures. This will include reviewing the organization's information protection procedures and related policies.
- Ensuring that POPI Reviews are scheduled and conducted on a regular basis.
- Ensuring that the organization makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to the organization. For instance, maintaining a "contact us" facility on the organization's website.
- Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by the organization. This will include overseeing the amendment of the organization's employment contracts and other service level agreements.
- Encouraging compliance with the conditions required for the lawful processing of personal information.
- Ensuring that employees and other persons acting on behalf of the organization are fully aware of the risks associated with the processing of personal information and that they remain informed about the organization's security controls.
- Organizing and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the organization.
- Addressing employees' POPIA related questions.
- Addressing all POPIA related requests and complaints made by the organization's data subjects.
- Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

The Deputy Information Officer will assist the Information Officer in performing his or her duties.

4.3 IT Manager

The organisation's IT Manager is responsible for:

- Ensuring that the organization's IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards.
- Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services.
- Ensuring that servers containing personal information are sited in a secure location, away from the general office space.
- Ensuring that all electronically stored personal information is backed-up and tested on a regular basis.
- Ensuring that all back-ups containing personal information are protected from unauthorized access, accidental deletion and malicious shacking attempts.
- Ensuring that personal information being transferred electronically is encrypted.
- Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software.
- Performing regular IT Reviews to ensure that the security of the organizations' hardware and software systems are functioning properly.
- Performing regular IT Reviews to verify whether electronically stored personal information has been accessed or acquired by any unauthorized persons.
- Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on the organizations' behalf. For instance, cloud computing services.

4.4 Marketing & Communication Manager

The organisation's Marketing & Communication Manager is responsible for:

- Approving and maintaining the protection of personal information statements and disclaimers that are displayed on the organization's website, including those attached to communications such as emails and electronic newsletters.
- Addressing any personal information protection queries from journalists or media outlets such as newspapers.
- Where necessary, working with persons acting on behalf of the organization to ensure that any outsourced marketing initiatives comply with POPIA.

4.5 Employees and other Persons acting on behalf of the Organisation

Employees and other persons acting on behalf of the organisation will, during the course of the performance of their services, gain access to and become acquainted with the personal information of certain customers/clients/donors/visitors/beneficiaries/suppliers and other employees.

Employees and other persons acting on behalf of the organisation are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

Employees and other persons acting on behalf of the organisation may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the organisation or externally, any personal information, unless such information is already publicly known, or the disclosure is necessary in order for the employee or person to perform his or her duties.

Employees and other persons acting on behalf of the organisation must request assistance from their line manager or the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.

Employees and other persons acting on behalf of the organisation will only process personal information where:

- The data subject, or a competent person where the data subject is a child, consents to the processing; or
- The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or
- The processing complies with an obligation imposed by law on the responsible party; or
- The processing protects a legitimate interest of the data subject; or

- The processing is necessary for pursuing the legitimate interests of the organization or of a third party to whom the information is supplied.

Furthermore, personal information will only be processed where the data subject:

- Clearly understands why and for what purpose his, her or its personal information is being collected; and
- Has granted the organization with explicit written or verbally recorded consent to process his, her or its personal information.

Employees and other persons acting on behalf of the organisation will consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.

Informed consent is therefore when the data subject clearly understands for what purpose his, her or its personal information is needed and who it will be shared with.

Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, the organisation will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.

Consent to process a data subject's personal information will be obtained directly from the data subject, except where:

- the personal information has been made public, or
- where valid consent has been given to a third party, or
- the information is necessary for effective law enforcement.

Employees and other persons acting on behalf of the organisation will under no circumstances:

- Process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties.
- Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All personal information must be accessed and updated from the organizations' central database or a dedicated server.
- Share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure. Where access to personal information is required, this may be requested from the relevant line manager or the Information Officer.
- Transfer personal information outside of South Africa without the express permission from the Information Officer.

Employees and other persons acting on behalf of the organisation are responsible for:

- Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.
- Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.
- Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The IT Manager will assist employees and where required, other persons acting on behalf of the organization, with the sending or sharing of personal information to or with authorized external persons.
- Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorized persons.
- Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.
- Ensuring that where personal information is stored on removable storage medias such as external drives, CDs or DVDs that these are kept locked away securely when not being used.
- Ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorized people cannot access it. For instance, in a locked drawer of a filing cabinet.
- Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorized individuals could see or copy them. For instance, close to the printer.
- Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the customers/clients/donors/visitors/beneficiaries' phone or communicates via email. Where a data subject's information is found to be out of date, authorization must first be obtained from the relevant line manager or the Information Officer to update the information accordingly.

- Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorization must first be obtained from the relevant line manager or the Information Officer to delete or dispose of the personal information in the appropriate manner.
- Undergoing POPI Awareness training from time to time.

Where an employee, or a person acting on behalf of the organisation, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer or the Deputy Information Officer.

5. PROCESSING OF PERSONAL INFORMATION

5.1. Purpose of Processing

KENSINGTON HOME FOR THE AGED uses the Personal Information under its care in the following ways:

- Conducting credit reference checks and assessments
- Identifying and managing its customers/clients/donors/visitors/beneficiaries/suppliers
- Identifying customers/clients/donors/visitors/beneficiaries/suppliers medical and other related health needs
- Administration of agreements
- Providing products and services to customers/clients/donors/visitors/beneficiaries/suppliers
- Detecting and prevention of fraud, crime, money laundering and other malpractice
- Conducting market or customers/clients/donors/visitors/beneficiaries/suppliers satisfaction research
- Marketing and sales
- In connection with legal proceedings
- Staff administration
- Keeping of accounts and records
- Complying with legal and regulatory requirements
- Profiling data subjects for the purposes of direct marketing
- Fundraising
- Beneficiary information to be provided to relevant Government or Funding Bodies

5.2. Personal information Collected

Section 9 of POPI states that *"Personal Information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive."*

KENSINGTON HOME FOR THE AGED collects and processes client/donors/beneficiaries' personal information pertaining to the needs of the business. The type of information of information will depend on the needs for which it is collected and will be processed for that purpose only. Whenever possible, **KENSINGTON HOME FOR THE AGED** will inform the client/donors/beneficiaries as to the information required and the information deemed optional. **KENSINGTON HOME FOR THE AGED** aims to have agreements in place with all product suppliers, insurers and third-party service providers to ensure a mutual understanding with regard to protection of the customer/client/donor/visitor/beneficiary/suppliers' personal information. With the customer/client/donor/visitor/beneficiary/suppliers' consent, **KENSINGTON HOME FOR THE AGED** may also supplement the information provided with the information that it receives from other providers in order to offer a more consistent and personalized experience for its clients/donors/beneficiaries'.

5.3. Categories of Data Subjects and their Personal Information

KENSINGTON HOME FOR THE AGED may possess records relating to suppliers, shareholders, contractors service providers, staff', customers, beneficiaries, donors and relevant Government/Funding Bodies:

Entity Type	**Personal Information Processed**
Customers/clients/donors/visitors/beneficiaries: Natural Persons	Names; contact details; physical and postal addresses; date of birth; ID number; tax related information; nationality; gender; confidential correspondence; medical information
Customer – Juristic Persons / Entities	Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax related information; authorized signatories; beneficiaries; ultimate beneficial owners; shareholding information; BBBEE information
Contracted Service Providers	Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax related information; authorized signatories; beneficiaries; ultimate beneficial owners; shareholding information; BBBEE information
Donors (Fundraising)	Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax related information; authorized signatories; beneficiaries; ultimate beneficial owners; shareholding information; BBBEE information
Employees / Directors	Gender; pregnancy; marital status; colour, race; age; language; education information; financial information; employment history; ID number; physical and postal address; contact details; opinions; criminal record; well-being

5.4. Categories of Recipients for Processing the Personal Information

KENSINGTON HOME FOR THE AGED may share the Personal Information with its agents, affiliates, and associated companies or Government Bodies who may use this information to send the Data Subject information on products and services. **KENSINGTON HOME FOR THE AGED** may supply the Personal Information to any party to whom **KENSINGTON HOME FOR THE AGED** may have assigned or transferred any of its rights or obligations under any agreement, and/or to service providers who render the following services:

- Capturing and organizing of data;
- Storing of data;
- Sending of emails and other correspondence to customers/clients/donors/visitors/beneficiaries/suppliers and relevant Government/Funding Bodies;
- Conducting due diligence checks;

5.5. Retention of Personal Information Records

KENSINGTON HOME FOR THE AGED may retain Personal Information records indefinitely, unless the Data Subject objects thereto. If the Data Subject objects to indefinite retention of its Personal Information **KENSINGTON HOME FOR THE AGED** shall retain the Personal Information records to the extent permitted or required by law.

5.6. General Description of Information Security Measures

KENSINGTON HOME FOR THE AGED employs up to date technology to ensure the confidentiality, integrity and availability of the Personal Information under its care. Measures include:

- Firewalls
- Virus protection software and update protocols
- Logical and physical access control;
- Secure setup of hardware and software making up the IT infrastructure;
- Outsourced Service Providers who process Personal Information on behalf of **KENSINGTON HOME FOR THE AGED** are contracted to implement security controls;
- Personal information shall be stored on site and access shall be limited to authorized personal only.
- All electronic files or data shall be backed up on to cloud based services.

6. ACCESS TO PERSONAL INFORMATION

All individuals and entities may request access, amendment, or deletion of their own Personal Information held by **KENSINGTON HOME FOR THE AGED**. Any requests should be directed, on the prescribed form, to the Information Officer.

6.1. Remedies available if request for access to Personal Information is refused

6.1.1. Internal Remedies

KENSINGTON HOME FOR THE AGED does not have internal appeal procedures. As such, the decision made by the Information Officer pertaining to a request is final, and requestors will have to exercise such external remedies at their disposal if a request is refused, and the requestor is not satisfied with the response provided by the information officer.

6.1.2. External Remedies

A requestor that is dissatisfied with the information officer's refusal to disclose information, may within 30 days of notification of the decision, apply to a court for relief. Likewise, a third party dissatisfied with the information officer's decision to grant a request for information, may within 30 days of notification of the decision, apply to a court for relief. For purposes of the Act, courts that have jurisdiction over these applications are the Constitutional Court, the High Court or another

court of similar status.

6.2. Grounds for Refusal

KENSINGTON HOME FOR THE AGED may legitimately refuse to grant access to a requested record that falls within a certain category. Grounds on which **KENSINGTON HOME FOR THE AGED** may refuse access include:

- Protecting personal information that **KENSINGTON HOME FOR THE AGED** holds about a third person (who is a natural person) including a deceased person, from unreasonable disclosure;
- Protecting commercial information that **KENSINGTON HOME FOR THE AGED** holds about a third party or **KENSINGTON HOME FOR THE AGED** (for example trade secret: financial, commercial, scientific or technical information that may harm the commercial or financial interests of the organization or the third party);
- If disclosure of the record would result in a breach of a duty of confidence owed to a third party in terms of an agreement;
- If disclosure of the record would endanger the life or physical safety of an individual;
- If disclosure of the record would prejudice or impair the security of property or means of transport;
- If disclosure of the record would prejudice or impair the protection of a person in accordance with a witness protection scheme;
- If disclosure of the record would prejudice or impair the protection of the safety of the public;
- The record is privileged from production in legal proceedings, unless the legal privilege has been waived;
- Disclosure of the record (containing trade secrets, financial, commercial, scientific, or technical information) would harm the commercial or financial interests of **KENSINGTON HOME FOR THE AGED**;
- Disclosure of the record would put **KENSINGTON HOME FOR THE AGED** at a disadvantage in contractual or other negotiations or prejudice it in commercial competition;
- The record is a computer programme; and
- The record contains information about research being carried out or about to be carried out on behalf of a third party or **KENSINGTON HOME FOR THE AGED**.

Records that cannot be found or do not exist

If **KENSINGTON HOME FOR THE AGED** has searched for a record and it is believed that the record does not exist or cannot be found, the requester will be notified by way of an affidavit or affirmation. This will include the steps that were taken to try to locate the record.

7. IMPLEMENTATION GUIDELINES

7.1. Training & Dissemination of Information

This Policy has been put in place throughout **KENSINGTON HOME FOR THE AGED**, training on the Policy and POPI will take place with all affected employees.

All new employees will be made aware at induction, or through training programmes, of their responsibilities under the terms of this Policy and POPI.

Modifications and updates to data protection and information sharing policies, legislation, or guidelines will be brought to the attention of all staff.

7.2. Employee Contracts

Each new employee will sign an Employment Contract containing the relevant consent clauses for the use and storage of employee information, and a confidentiality undertaking as part and will be personally responsible for ensuring there are no breaches of confidentiality in relation to any Personal Information, however it is stored. Failure to comply will result in the instigation of a disciplinary procedure.

Each employee currently employed within **KENSINGTON HOME FOR THE AGED** will sign an addendum to their Employment Contract containing the relevant consent clauses for the use and storage of employee information, and a confidentiality undertaking as part and will be personally responsible for ensuring there are no breaches of confidentiality in relation to any Personal Information, however it is stored. Failure to comply will result in the instigation of a disciplinary procedure.

8. EIGHT PROCESSING CONDITIONS

POPI is implemented by abiding by eight processing conditions. **KENSINGTON HOME FOR THE AGED** shall abide by these principles in all its possessing activities.

8.1. Accountability

KENSINGTON HOME FOR THE AGED shall ensure that all processing conditions, as set out in POPI, are complied with when determining the purpose and means of processing Personal Information and during the processing itself. **KENSINGTON HOME FOR THE AGED** shall remain liable for compliance with these conditions, even if it has outsourced it processing activities.

8.2. Processing Limitation

8.2.1 Lawful grounds

The processing of Personal Information is only lawful if, given the purpose of processing, the information is adequate, relevant and not excessive.

KENSINGTON HOME FOR THE AGED may only process Personal Information if one of the following grounds of lawful processing exists:

- The Data Subject consents to the processing;
- Processing is necessary for the conclusion or performance of a contract with the Data Subject;
- Processing complies with a legal responsibility imposed on **KENSINGTON HOME FOR THE AGED**;
- Processing protects a legitimate interest of the Data Subject;
- Processing is necessary for pursuance of a legitimate interest of **KENSINGTON HOME FOR THE AGED**, or a third party to whom the information is supplied;

Special Personal Information includes:

- Religious, philosophical, or political beliefs;
- Race or ethnic origin;
- Trade union membership;
- Health or sex life;
- Biometric information (including blood type, fingerprints, DNA, retinal scanning, voice recognition, photographs);
- Criminal behavior;
- Information concerning a child.

KENSINGTON HOME FOR THE AGED may only process Special Personal Information under the following circumstances:

- The Data Subject has consented to such processing;
- The Special Personal Information was deliberately made public by the Data Subject;
- Processing is necessary for the establishment of a right or defence in law;
- Processing is for historical, statistical, or research reasons
- If processing of race or ethnic origin is in order to comply with affirmative action laws

All Data Subjects have the right to refuse or withdraw their consent to the processing of their Personal Information, and a Data Subject may object, at any time, to the processing of their

Personal Information on any of the above grounds, unless legislation provides for such processing. If the Data subject withdraws consent or objects to processing then **KENSINGTON HOME FOR THE AGED** shall forthwith refrain from processing the Personal Information.

8.2.2. Collection directly from the Data Subject

Personal Information must be collected directly from the Data Subject, unless:

- Personal Information is contained in a public record;
- Personal Information has been deliberately made public by the Data Subject;
- Personal Information is collected from another source with the Data Subject's consent;
- Collection of Personal Information from another source would not prejudice the Data Subject;
- Collection of Personal Information from another source is necessary to maintain, comply with or exercise any law or legal right;
- Collection from the Data Subject would prejudice the lawful purpose of collection;
- Collection from the Data Subject is not reasonably practicable.

8.3. Purpose Specification

KENSINGTON HOME FOR THE AGED shall only process Personal Information for the specific purposes as set out and defined above herein.

8.4. Further Processing

New processing activity must be compatible with original purpose of processing. Further processing will be regarded as compatible with the purpose of collection if:

- Data Subject has consented to the further processing;
- Personal Information is contained in a public record;
- Personal Information has been deliberately made public by the Data Subject;
- Further processing is necessary to maintain, comply with or exercise any law or legal right;
- Further processing is necessary to prevent or mitigate a threat to public health or safety, or the life or health of the Data Subject or a third party

8.5. Information Quality

KENSINGTON HOME FOR THE AGED shall take reasonable steps to ensure that Personal Information is complete, accurate, not misleading and updated. **KENSINGTON HOME FOR THE AGED** shall periodically review Data Subject records to ensure that the Personal Information is still valid and correct.

Employees should as far as reasonably practicable follow the following guidance when collecting Personal Information:

- Personal Information should be dated when received;
- A record should be kept of where the Personal Information was obtained;
- Changed to information records should be dated;
- Irrelevant or unneeded Personal Information should be deleted or destroyed;
- Personal Information should be stored securely, either on a secure electronic database or in a secure physical filing system.

8.6. Openness

KENSINGTON HOME FOR THE AGED shall take reasonable steps to ensure that the Data Subject is made aware of:

- What Personal Information is collected, and the source of the information;
- The purpose of collection and processing;
- Where the supply of Personal Information is voluntary or mandatory, and the consequences of a failure to provide such information;

- Whether collection is in terms of any law requiring such collection;
- Whether the Personal Information shall be shared with any third party.

8.7. Data Subject Participation

Data Subject have the right to request access to, amendment, or deletion of their Personal Information.
All such requests must be submitted in writing to the Information Officer. Unless there are grounds for refusal as set out in paragraph 7.2, above, **KENSINGTON HOME FOR THE AGED** shall disclose the requested Personal Information:

- On receipt of adequate proof of identity from the Data Subject, or requester;
- Within a reasonable time;
- On receipt of the prescribed fee, if any;
- In a reasonable format

KENSINGTON HOME FOR THE AGED shall not disclose any Personal Information to any party unless the identity of the requester has been verified.

8.8. Security Safeguards

KENSINGTON HOME FOR THE AGED shall ensure the integrity and confidentiality of all Personal Information in its possession, by taking reasonable steps to:

- Identify all reasonably foreseeable risks to information security;
- Establish and maintain appropriate safeguards against such risks;

8.8.1. Written records

- Personal Information records should be kept in locked cabinets, or safes;
- When in use Personal Information records should not be left unattended in areas where non-staff members may access them;
- **KENSINGTON HOME FOR THE AGED** shall implement and maintain a “Clean Desk Policy” where all employees shall be required to clear their desks of all Personal Information when leaving their desks for any length of time and at the end of the day;
- Personal Information which is no longer required should be disposed of by shredding.

Any loss or theft of, or unauthorized access to, Personal Information must be immediately reported to the Information Officer.

8.8.2. Electronic Records

- All electronically held Personal Information must be saved in a secure database;
- As far as reasonably practicable, no Personal Information should be saved on individual computers, laptops or hand-held devices;
- All computers, laptops and hand-held devices should be access protected with a password, fingerprint or retina scan, with the password being of reasonable complexity and changed frequently;
- **KENSINGTON HOME FOR THE AGED** shall implement and maintain a “Clean Screen Policy” where all employees shall be required to lock their computers or laptops when leaving their desks for any length of time and to log off at the end of the day;
- Electronical Personal Information which is no longer required must be deleted from the individual laptop or computer and the relevant database. The employee must ensure that the information has been completely deleted and is not recoverable.

Any loss or theft of computers, laptops or other devices which may contain Personal Information must be immediately reported to the Information Officer, who shall notify the IT department, who shall take all necessary steps to remotely delete the information, if possible.

9. DIRECT MARKETING & FUNDRAISING

All Direct Marketing and Fundraising communications shall contain **KENSINGTON HOME FOR THE AGED**'s, and/or the Non-Profit's details, and an address or method for the customers/clients/donors/visitors/beneficiaries/suppliers to opt-out of receiving further marketing communication.

9.1.1. Existing customers/clients/donors/visitors/beneficiaries/suppliers

Direct Marketing by electronic means to existing customers/clients/donors/visitors/beneficiaries/suppliers is only permitted:

- If the customers/clients/donors/visitors/beneficiaries/suppliers' details were obtained in the context of a sale or service; and
- For the purpose of marketing the same or similar products;

The customers/clients/donors/visitors/beneficiaries/suppliers must be given the opportunity to opt-out of receiving direct marketing on each occasion of direct marketing.

9.1.2. Consent

KENSINGTON HOME FOR THE AGED may send electronic Direct Marketing communication to Data Subjects who have consented to receiving it. **KENSINGTON HOME FOR THE AGED** may approach a Data Subject for consent only once.

9.1.3. Record Keeping

KENSINGTON HOME FOR THE AGED shall keep record of:

9.1.3.1. Date of consent
9.1.3.2. Wording of the consent
9.1.3.3. Who obtained the consent
9.1.3.4. Proof of opportunity to opt-out on each marketing contact
9.1.3.5. Record of opt-outs

10. DESTRUCTION OF DOCUMENTS

10.1. Documents may be destroyed after the termination of the retention period specified herein, or as determined by the Non-Profit from time to time.

10.2. Each department is responsible for attending to the destruction of its documents and electronic records, which must be done on a regular basis. Files must be checked in order to make sure that they may be destroyed and also to ascertain if there are important original documents in the file. Original documents must be returned to the holder thereof, failing which, they should be retained by the Non-Profit pending such return.

10.3. The documents must made available for collection by the shredding company, or other approved document disposal company.

10.4. Deletion of electronic records must be done in consultation with the IT Department, to ensure that deleted information is incapable of being reconstructed and/or recovered.

11. STATUTORY RETENTION PERIODS

Legislation	Document Type	Period
Companies Act	Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Act; Notice and minutes of all shareholders meeting, including resolutions adopted and documents made available to holders of securities; Copies of reports presented at the annual general meeting of the company; Copies of annual financial statements required by the Act; Copies of accounting records as required by the Act; Record of directors and past directors, after the director has retired from the company; Written communication to holders of securities and Minutes and resolutions of directors' meetings, audit committee and directors' committees.	7 Years

	Registration certificate; Memorandum of Incorporation and alterations and amendments; Rules; Securities register and uncertified securities register; Register of company secretary and auditors and Regulated Companies (companies to which chapter 5, part B, C and Takeover Regulations apply) – Register of disclosure of person who holds beneficial interest equal to or in excess of 5% of the securities of that class issued.	Indefinitely

Consumer Protection Act	Full names, physical address, postal address and contact details; ID number and registration number; Contact details of public officer in case of a juristic person; Service rendered; Cost to be recovered from the consumer; Frequency of accounting to the consumer; Amounts, sums, values, charges, fees, remuneration specified in monetary terms; Conducting a promotional competition refer to Section 36(11)(b) and Regulation 11 of Promotional Competitions;	3 years

Financial Intelligence Centre Act	Whenever a reportable transaction is concluded with a customer/client/donor/visitor/beneficiary/supplier, the institution must keep record of the identity of the customer/client/donor/visitor/beneficiary/supplier; If the customer/client/donor/visitor/beneficiary/supplier is acting on behalf of another person, the identity of the person on whose behalf the customer/client/donor/visitor/beneficiary/supplier is acting and the customer/client/donor/visitor/beneficiary/supplier authority to act on behalf of that other person; If another person is acting on behalf of the customer/client/donor/visitor/beneficiary/supplier, the identity of that person and that other person's authority to act on behalf of the customer/client/donor/visitor/beneficiary/supplier; The manner in which the identity of the persons referred to above was established; The nature of that business relationship or transaction; In the case of a transaction, the amount involved and the parties to that transaction; All accounts that are involved in the transactions concluded by that accountable institution in the course of that business relationship and that single transaction; The name of the person who obtained the identity of the person transacting on behalf of the accountable institution; Any document or copy of a document obtained by the accountable institution	5 years

Compensation for Occupational Injuries and Diseases Act	Register, record or reproduction of the earnings, time worked, payment for piece work and overtime and other prescribed particulars of all the employees.	4 years
	Section 20(2) documents : -Health and safety committee recommendations made to an employer in terms of issues affecting the health of employees and of any report made to an inspector in terms of the recommendation; -Records of incidents reported at work.	3 years
	Asbestos Regulations, 2001, regulation 16(1): -Records of assessment and air monitoring, and the asbestos inventory; -Medical surveillance records; Hazardous Biological Agents Regulations, 2001, Regulations 9(1) and (2): -Records of risk assessments and air monitoring; -Medical surveillance records. Lead Regulations, 2001, Regulation 10: -Records of assessments and air monitoring; -Medical surveillance records Noise - induced Hearing Loss Regulations, 2003, Regulation 11: -All records of assessment and noise monitoring; -All medical surveillance records, including the baseline audiogram of every employee.	40 years
	Hazardous Chemical Substance Regulations, 1995, Regulation 9: -Records of assessments and air monitoring; -Medical surveillance records	30 years

Basic Conditions of Employment Act	Section 29(4): -Written particulars of an employee after termination of employment; Section 31: -Employee's name and occupation; -Time worked by each employee; -Remuneration paid to each employee; -Date of birth of any employee under the age of 18 years.	3 years
Employment Equity Act	Records in respect of the organisations' workforce, employment equity plan and other records relevant to compliance with the Act; Section 21 report which is sent to the Director General	3 years
Labour Relations Act	Records to be retained by the employer are the collective agreements and arbitration awards.	3 years
	An employer must retain prescribed details of any strike, lock-out or protest action involving its employees; Records of each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and the reasons for the actions	Indefinite
Unemployment Insurance Act	Employers must retain personal records of each of their current employees in terms of their names, identification number, monthly remuneration and address where the employee is employed	5 years
Tax Administration Act	Section 29 documents which: -Enable a person to observe the requirements of the Act; -Are specifically required under a Tax Act by the Commissioner by the public notice; -Will enable SARS to be satisfied that the person has observed these requirements	5 years

Income Tax Act	Amount of remuneration paid or due by him to the employee; The amount of employees tax deducted or withheld from the remuneration paid or due; The income tax reference number of that employee; Any further prescribed information; Employer Reconciliation return.	5 years
Value Added Tax Act	Where a vendor's basis of accounting is changed the vendor shall prepare lists of debtors and creditors showing the amounts owing to the creditors at the end of the tax period immediately preceding the changeover period; Importation of goods, bill of entry, other documents prescribed by the Custom and Excise Act and proof that the VAT charge has been paid to SARS; Vendors are obliged to retain records of all goods and services, rate of tax applicable to the supply, list of suppliers or agents, invoices and tax invoices, credit and debit notes, bank statements, deposit slips, stock lists and paid cheques; Documentary proof substantiating the zero rating of supplies; Where a tax invoice, credit or debit note, has been issued in relation to a supply by an agent or a bill of entry as described in the Customs and Excise Act, the agent shall maintain sufficient records to enable the name, address and VAT registration number of the principal to be ascertained.	5 years

Non-Profit Act	Keep and preserve accounting records and supporting documentation for the prescribed period. (Sections 17 (1)(a) and (3).	