



BDM
PROPERTY
MANAGEMENT

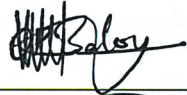


POLICY NAME

PROTECTION OF PERSONAL INFORMATION
POLICY (POPIA)

POLICY OWNER

THE BOARD OF DIRECTORS

APPROVAL PROCESS

POSITIONS	NAME	SIGNATURE	DATE
CHIEF EXECUTIVE OFFICER	OUPA PIET BALOYI		10 AUGUST 2021
CHIEF OPERATIONS OFFICER	MPEILE DISEGO DEBEILA		10 AUGUST 2021
CHIEF FINANCIAL OFFICER	ALBERT TLOU MOHOLOLA		10 AUGUST 2021





BDM
PROPERTY
MANAGEMENT



<i>Rule</i>	<i>Heading</i>	<i>Page</i>
1.	Policy statement	3
2.	Introduction	3
3.	Definitions	4
4.	Purpose of the policy	7
5.	Policy application	8
6.	General guiding principles	9
7.	What information do we process	9
8.	How is the Personal Information collected	11
9.	Circumstances when information is shared	11
10.	Data privacy statement	12
11.	Rights of data subjects	13
12.	Information officer	14
13.	Key roles and responsibilities	15
14.	Request for Personal Information procedure	22
15.	POPI complaints procedures	22
16.	Changes to the policy	24
17.	Implementation	24



BDM
PROPERTY
MANAGEMENT



1. POLICY STATEMENT

- 1.1. This policy forms part of the policy owner's internal business processes and procedures.
- 1.2. Any reference to the "organisation" shall be interpreted to include the "policy owner".
- 1.3. The organisation's governing body, its employees, volunteers, contractors, suppliers and any other persons acting on behalf of the organisation are required to familiarise themselves with the policy's requirements and undertake to comply with the stated processes and procedures.
- 1.4. Risk owners and control owners are responsible for overseeing and maintaining control procedures and activities.

2. INTRODUCTION

- 2.1. BDM Property management agency (referred to as "BDM"), is a management agency profit Company as defined in Section 1 of the Companies Act no 71 of 2008 which specializes with the management of sectional schemes and Homeowners Association.
- 2.2. The right to privacy is an integral human right recognised and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 ("POPIA")
- 2.3. POPIA aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in context-sensitive manner.
- 2.4. BDM is obliged to comply with The Protection of Personal Information Act ('POPIA') and given the importance of privacy, the body corporate is committed to effectively managing personal information in accordance with the Act.
- 2.5. POPI requires the trustees and the managing agent to inform owners, residents and service providers as to how their Personal Information is used, disclosed and destroyed.
- 2.6. BDM guarantees its commitment to protecting owners, residents and service providers' privacy and ensuring that their Personal Information is used appropriately, transparently, securely and in accordance with applicable laws.



BDM
PROPERTY
MANAGEMENT



- 2.7. This Policy sets out how the Company deals with the members and service providers' Personal Information and, in addition, the purposes said information is used for. This Policy is made available to all members and service providers by request from our Information Officer, whose details are provided in this document.
- 2.8. 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."

3. DEFINITIONS

All definitions contained in the Protection of Personal Information Act, Act 4 of 2013 apply to this Policy, with specific reference to:

- 3.1. **"Act and/or POPI"** - The Protection of Personal Information Act, Act 4 of 2013.
- 3.2. **"Board"** - means the board of directors of the Company, as appointed at the Elective Annual General Meeting (AGM);
- 3.3. **"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.
- 3.4. **"Consent"** - Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
- 3.5. **"Competent person"** - means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child;
- 3.6. **"Data subject"** - means the person to whom the personal information relates, including but not limited to the following owners, tenants, employees, visitors, contractors, and other relevant parties.



BDM
PROPERTY
MANAGEMENT



- 3.7. **“Direct Marketing”** – Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:
- a) Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or
 - b) Requesting the data subject to make a donation of any kind for any reason.
- 3.8. **“Information officer”** means:
- c) The person responsible for ensuring the Company’s compliance with POPIA;
 - d) The head of a body of the Company/organization.
 - e) Where no Information Officer is appointed, the head of a body of the Company will be responsible for performing the Information Officer’s duties.
 - f) 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.
- 3.9. **“Legitimate purpose”** – means for the operational, administrative, control, security, and any other objective of the Company in accordance with the Companies Act or its Memorandum of Incorporation, Constitution and/or founding documents.
- 3.10. **“Person”** – means a natural person or a juristic person;
- 3.11. **“Personal Information”** – means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to —
- a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or



BDM
PROPERTY
MANAGEMENT



- mental health, well-being, disability, religion, conscience, belief, culture, language, and birth of the person;
- b) information relating to the education or the medical, financial, criminal or employment history of the person;
 - c) any identifying number, symbol, email address, physical address, telephone number, location information, online identifier, or other particular assignments to the person;
 - d) the biometric information of the person;
 - e) the personal opinions, views, or preferences of the person;
 - f) 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;
 - g) the views or opinions of another individual about the person; and
 - h) 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;

3.12. **“Processing”**- means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—

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

3.13. **“PAIA”** - Promotion of Access to Information Act, Act 2 of 2000.

3.14. **“The head of Body”** – President, Chairperson, Managing Director or Chair of the Board, or a Business Rescue Practitioner in terms of the Companies Act.



BDM
PROPERTY
MANAGEMENT

- 3.15. **“Record”** - Means any recorded information, regardless of form or medium, including:
- a) Writing on any material;
 - b) 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;
 - c) Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
 - d) Book, map, plan, graph or drawing;
 - e) 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.
- 3.16. **“Responsible party”** – means a person who processes personal information of the Company, for example, employees, auditors, Attorneys, and alike.

4. PURPOSE OF THIS POLICY

- 4.1. The Protection of Personal Information (POPI) policy is intended to protect the personal information and special personal information of members, employees, service providers, and other relevant parties that is being processed by the Company's for the purpose of carrying on its objectives as defined in the Companies Act and/or its Constitution and/or Memorandum of Incorporation and/or founding documents and further ensures that this information is used for legitimate reasons and purpose.
- 4.2. Furthermore, this policy is intended to protect the Company from the compliance risks associated with the protection of personal information which includes:



BDM
PROPERTY
MANAGEMENT



- a) Breaches of confidentiality - For instance, the Company could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.
- b) Failing to offer choice - For instance, all data subjects should be free to choose how and for what purpose the Company uses information relating to them.
- c) Reputational damage - For instance, the Company could suffer the consequences of a reputational damage following an adverse event such as a computer hacker deleting the personal information held by the Company.

4.3. In addition to the above, this Policy provides for the minimum threshold of requirements for information held by all responsible parties that store and process information on behalf of the Company.

5. POLICY APPLICATION

5.1. This policy and its guiding principles applies to:

- a) The board of directors
- b) All employees and volunteers
- c) All contractors, suppliers and other persons acting on behalf of the organisation

5.2. The policy's guiding principles is applicable in all situations and must be read in conjunction with POPI Act (Act No 4 of 2013) as well as the organisation's PAIA Policy as required by the Promotion of Access to Information Act (Act No 2 of 2000).

5.3. The legal duty to comply with POPIA's provisions is activated in any situation where there is:

- A processing of.....
-personal information.....
-entered into a record.....
-by or for a responsible person.....
-who is domiciled in South Africa.



BDM
PROPERTY
MANAGEMENT

6. GENERAL GUIDING PRINCIPLES

6.1. POPI is based on eight conditions for the lawful processing of personal information and under each condition; there are a number of key requirements.

- a) Accountability - Personal information must be processed lawfully and in a reasonable manner. It should not infringe on any person's privacy outside of a legal or agreed to purpose.
- b) Processing limitation - The processing of personal information should always be relevant and never excessive. POPI provides for particular circumstances under which personal data may be processed. As such, the data subject's consent should be obtained before his or her information is processed.
- c) Purpose specification - Personal information may only be collected for a specific, lawful and explicitly defined purpose that relates to the data collector's function or activity. Information may not be retained for any longer than is absolutely necessary.
- d) Further processing limitation - Any further processing of personal information must be related to the purpose for which the information was originally collected.
- e) Information quality - A reasonable party must ensure that any personal information collected is complete, accurate, truthful and updated.
- f) Openness - A responsible party must document its process of collecting information as required by POPI's provisions. Data subjects must be notified or informed of how and when their personal information will be processed.
- g) Security safeguards - Personal information must be kept confidential and its integrity maintained. Responsible parties must take appropriate measures to guard any personal information against unlawful acts and to prevent its loss, damage or destruction.
- h) Data subject participation - Data subjects must be able to confirm whether or not an Company holds any of their personal information. They must also be allowed to correct their information or to request that the responsible party destroy or delete it.

7. WHAT INFORMATION DO WE PROCESS

7.1. The following information is processed in the Company for effective scheme management:



BDM
PROPERTY
MANAGEMENT



- a) Names, contact information, including email addresses, telephone numbers, physical address, postal address, and other location information including unit number or erven number.
- b) Birth date, age, gender, race, nationality, title and language preferences.
- c) Identity number, passport number and photograph.
- d) Employee numbers.
- e) Vehicle registration number, vehicle licence and driving license.
- f) Biometric information, including but not limited to, if applicable, information obtained from fingerprints, video, film, facial recognition and/or retinal scanning.
- g) Verified banking details.
- h) Employment details.
- i) Correspondence of a private or confidential nature.
- j) Personal information as defined above.
- k) Any other personal information, which is reasonably required to engage and provide services to the data subject effectively.

7.2. These records of the personal information about the members are processed in order to:

- a) Send accounts and statements to the correct people;
- b) Allocate payments correctly;
- c) Send out communications about the annual budget, the AGM and other Company meetings;
- d) Facilitate communications with members regarding organisational issues or in an emergency such as the recent Covid-19 lockdown; and
- e) Take swift action in the event of levy defaults, violations and transgressions
- f) Formulation of the WhatsApp groups and Facebook pages where at least some member information is shared
- g) In addition, the Company has controlled-access points where employees and visitors alike must provide personal information to gain entry to the building or to obtain a remote control or access card. This may include a car registration number,





BDM
PROPERTY
MANAGEMENT



a fingerprint and a photograph, for example, as well as their name and telephone number.

8. HOW IS THE PERSONAL INFORMATION COLLECTED

- 8.1. Personal information may be collected in the following ways:
- a) Directly from the data subject or its Agents
 - b) During the data subject's interaction with the Company
 - c) When data subjects visit the Company
 - d) When a data subject interacts with the Company on a virtual platform (i.e., website, social media, and or IT services)
 - e) From public records
 - f) From third parties who are authorised to share personal information
 - g) From mobile or software apps developed by the Company for legitimate purposes.

9. CIRCUMSTANCES WHEN PERSONAL INFORMATION IS SHARED

- 9.1. POPIA requires that personal information "is collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party."
- 9.2. Personal information may be processed in the following circumstances:
- a) When consent has been obtained from the data subject,
 - b) When there is a legitimate and lawful reason;
 - c) When processing is necessary for the safety and security of the members of the Company
 - d) When it is required in terms of law to ensure the proper functioning of the Company
- 9.3. We may collect other personal information from time to time where you provide it to us, as necessary for our business requirements, or in order to comply with applicable laws.



BDM
PROPERTY
MANAGEMENT



9.4. Depending on the above circumstances, the Company may disclose personal information to the following categories of responsible parties:

- a) Auditors, legal and other professional advisors and consultants of the Company or third parties assisting the Company in service delivery including but not limited to Professional bodies, Universities and Administrators.
- b) Information Technology and other service providers who assist in the effective running and management of the Company.
- c) Service providers who assist in the storing of personal information.
- d) Government and law enforcement authorities.
- e) Financial institutions
- f) Other third parties where disclosure is required by law or otherwise required for Company's to perform their obligations and provide services in accordance with the Companies Act or its Memorandum of Incorporation, Constitution and/or founding documents.
- g) To any other person with the consent of the data subject.
- h) Members of the Company in terms of Memorandum of Incorporation and/or any other Rule or right in terms of the founding documents

10. DATA PRIVACY STATEMENT

10.1. The following data privacy statement must appear on all documents related to the Company containing personal information:

"The organisation _____ undertakes to take reasonable steps to protect the confidentiality and security of the data subject's personal information when it is disclosed to a third party and seeks to ensure that the third-party deals with the personal information in accordance with the instructions of the Company, applicable privacy laws and used only for the purposes for which it is disclosed."



BDM
PROPERTY
MANAGEMENT



11. RIGHTS OF DATA SUBJECTS

11.1. Where appropriate, the organisation will ensure that its clients and customers are made aware of the rights conferred upon them as data subjects.

11.2. The organisation will ensure that it gives effect to the following rights of data subjects:

a) The Right to Access Personal Information

- The organisation recognises that a data subject has the right to establish whether the organisation holds personal information related to him, her or it including the right to request access to that personal information.
- An example of a "Personal Information Request Form" can be found under Annexure A.

b) The Right to have Personal Information Corrected or Deleted

- The data subject has the right to request, where necessary, that his, her or its personal information must be corrected or deleted where the organisation is no longer authorised to retain the personal information. Please contact BDM directly for assistance with this process.

c) The Right to Object to the Processing of Personal Information

- The data subject has the right, on reasonable grounds, to object to the processing of his, her or its personal information.
- In such circumstances, the organisation will give due consideration to the request and the requirements of POPIA. The organisation may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements approve the destruction of the personal information.
- Please contact BDM directly for assistance with this process.

d) The Right to Object to Direct Marketing

- The data subject has the right to object to the processing of his, her or its personal information for purposes of direct marketing by means of unsolicited electronic communications.
- Please contact BDM directly for assistance with this process.

e) The Right to Complain to the Information Regulator

- The data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and





BDM
PROPERTY
MANAGEMENT



to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information.

- To lodge a complaint with BDM, please complete the "POPI Complaint Form" that can be found under Annexure B and submit to our offices

f) The Right to be Informed

- The data subject has the right to be notified that his, her or its personal information is being collected by the organisation.
- The data subject also has the right to be notified in any situation where the organisation has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.
- Please contact BDM directly for assistance with this process.

11.3. Should the data subject wish to exercise any of the abovementioned rights or raise any queries regarding the personal information held, the data subject can contact the Company directly.

11.4. In the event that the data subject requires his/her personal information to be deleted, the Company may need to terminate all agreements with the data subject. The Company may refuse to delete the data subjects' personal information if required by law to retain it, or in the event it needs to protect its rights.

11.5. Should a data subject have any questions, concerns, or complaints regarding the way in which the Company handles the personal information, or if the data subject believes that the Company has failed to comply with this Policy or breached any applicable laws in relation to the management of that information, the data subject may issue a formal complaint.

11.6. Any question, concern or complaint should be made in writing to the head of the Company.

12. INFORMATION OFFICERS

12.1. The Company will appoint an Information Officer and where necessary, a Deputy Information Officer to assist the Information Officer.





BDM
PROPERTY
MANAGEMENT



- 12.2. The Company's Information Officer is responsible for ensuring compliance with POPIA.
- 12.3. There are no legal requirements under POPIA for the Company to appoint an Information Officer. Appointing an Information Officer is however, considered to be a good business practice, particularly within larger Company.
- 12.4. Where no Information Officer is appointed, the head of the head of the body will assume the role of the Information Officer. Consideration will be given on an annual basis to the re-appointment or replacement of the Information Officer and the re-appointment or replacement of any Deputy Information Officers.
- 12.5. The appointed information officer are as follows:

Information officer: Mpeile Disego Debeila

Email: Disego@bdmpm.co.za

Cell: 073 816 8785

13. KEY ROLES AND RESPONSIBILITIES

- 13.1. **The company's Board of directors** is responsible for ensuring that:
- a) The company appoints an Information Officer, and where necessary, a Deputy Information Officer.
 - b) All persons responsible for the processing of personal information on behalf of the organisation:
 - 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.
 - c) 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.



BDM
PROPERTY
MANAGEMENT

- d) The scheduling of a periodic POPI Audit in order to accurately assess and review the ways in which the organisation collects, holds, uses, shares, discloses, destroys and processes personal information.
- e) The Company meets its legal obligations in terms of POPIA and cannot delegate its accountability. The Board of directors may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

13.2. The Company's Information Officer is responsible for:

- a) Taking steps to ensure the Company's reasonable compliance with the provision of POPIA.
- b) Keeping the members updated about the Company's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the members of their obligations pursuant to POPIA.
- c) Continually analysing privacy regulations and aligning them with the Company's personal information processing procedures. This will include reviewing the Company's information protection procedures and related policies.
- d) Ensuring that the Company makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to the Company.
- e) Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by the Company. This will include overseeing the amendment of the Company's employment contracts and other service level agreements.
- f) Encouraging compliance with the conditions required for the lawful processing of personal information.
- g) Ensuring that employees and other persons acting on behalf of the Company are fully aware of the risks associated with the processing of personal information and that they remain informed about the Company's security controls.



BDM
PROPERTY
MANAGEMENT

- h) Addressing all POPIA related requests and complaints made by the Company's data subjects.
- i) 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.

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

13.4. **The Company's IT service** is responsible for:

- a) Ensuring that the organisation's IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards.
- b) Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services.
- c) Ensuring that servers containing personal information are sited in a secure location, away from the general office space.
- d) Ensuring that all electronically stored personal information is backed-up and tested on a regular basis.
- e) Ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious shacking attempts.
- f) Ensuring that personal information being transferred electronically is encrypted.
- g) Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software.
- h) Performing regular IT audits to ensure that the security of the organisation's hardware and software systems are functioning properly.
- i) Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons.



BDM
PROPERTY
MANAGEMENT

- j) Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on the organisation's behalf. For instance, cloud computing services.

13.5. The Communication Manager is responsible for:

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

13.6. Employees and other Persons acting on behalf of the Organisation

13.6.1. 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 members, certain clients, suppliers and other employees.

13.6.2. 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.

13.6.3. 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.

13.6.4. 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.



BDM
PROPERTY
MANAGEMENT

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

- a) The data subject, or a competent person where the data subject is a child, consents to the processing; or
- b) 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
- c) The processing complies with an obligation imposed by law on the responsible party; or
- d) The processing protects a legitimate interest of the data subject; or
- e) The processing is necessary for pursuing the legitimate interests of the organisation or of a third party to whom the information is supplied.

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

- a) clearly understands why and for what purpose his, her or its personal information is being collected; and
- b) has granted the organisation with explicit written or verbally recorded consent to process his, her or its personal information.

13.6.7. 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.

13.6.8. 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.

13.6.9. 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**





BDM
PROPERTY
MANAGEMENT



instances where transactions are concluded telephonically or via electronic video feed.

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

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

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

- a) 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.
- b) 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 organisation's central database or a dedicated server.
- c) 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.
- d) Transfer personal information outside of South Africa without the express permission from the Information Officer.

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

- a) Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.





BDM
PROPERTY
MANAGEMENT

- b) 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.
- c) Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The IT service will assist employees and where required, other persons acting on behalf of the organisation, with the sending or sharing of personal information to or with authorised external persons.
- d) 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 unauthorised persons.
- e) Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.
- f) 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.
- g) Ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer of a filing cabinet.
- h) Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer.
- i) 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 client or customer phones or communicates via email. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the Information Officer to update the information accordingly.





BDM
PROPERTY
MANAGEMENT

- j) 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, authorisation 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.
- k) Undergoing POPI Awareness training from time to time.

13.6.13. Where an employee, or a person acting on behalf of the Company, 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.

14. REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

14.1. Data subjects have the right to:

- a) Request what personal information the Company holds about them and why.
- b) Request access to their personal information.
- c) Be informed how to keep their personal information up to date.

14.2. Access to information requests can be made by email, addressed to the Information Officer. The Information Officer will provide **the data subject with a "Personal Information Request Form"**.

14.3. Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information. All requests will be processed and considered within a reasonable time.

15. POPI COMPLAINTS PROCEDURE



BDM
PROPERTY
MANAGEMENT

any decisions taken and communicate any anticipated deviation from the specified timelines.

h) The Information Officer's response to the data subject may comprise any of the following:

- i) A suggested remedy for the complaint,
 - ii) A dismissal of the complaint and the reasons as to why it was dismissed,
 - iii) An apology (if applicable) and any disciplinary action that has been taken against any members involved.
- i) Where the data subject is not satisfied with the Information Officer's suggested remedies, the data subject has the right to complain to the Information Regulator.
- j) The Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPI related complaints.

16. CHANGES TO POLICY

- 16.1. This Policy was published on [] and last updated on [].
- 16.2. The Company may change this Policy from time to time, and when so done, an electronic copy will be emailed to the data subjects.

17. IMPLEMENTATION

- 17.1. The signatories as indicated on page 1 of this policy confirm their acceptance of the contents and recommend the adoption of this Policy thereof.



BDM
PROPERTY
MANAGEMENT

15.1. Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. The Company takes all complaints very seriously and will address all POPI related complaints in accordance with the following procedure:

- a) POPI complaints must be submitted to the Company in writing. Where so required, the Information Officer will provide the **data subject with a "POPI Complaint Form"**.
- b) Where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within 2 working days.
- c) The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 5 working days.
- d) The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA.
- e) The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on the Company's data subjects.
- f) Where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised person, the Information Officer will consult with the Company trustee committee where after the affected data subjects and the Information Regulator will be informed of this breach.
- g) The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to the trustees within 7 working days of receipt of the complaint. In all instances, the Company will provide reasons for