The Body Corporate of St Martini Gardens SS249/2002

Privacy Policy

74 QUEEN VICTORIA ST., CAPE TOWN 8001, TEL: +27 (0) 21 424 7529, WWW.STMARTINIGARDENS.CO.ZA

1. Purpose of this policy

The trustees of St Martini Gardens (SMG) are aware of the need to protect the privacy of its members, residents, visitors, employees, service providers and the general public in line with the South African constitution and the Protection of Personal Information Act 2013 (POPIA).

This policy describes the way that the SMG Body Corporate (BC) (consisting of all members) will meet its obligations in terms of this legislation to protect the personal information it holds. The Policy applies to all members, trustees, employees, service providers and agents. The provisions of the Policy are applicable to both on and off-site processing of personal information.

2. Definitions

Consent	Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
Data Subject	This refers to the natural or juristic person to whom personal information relates. In terms of SMG this may be residents, owners, visitors, employees, service providers and the general public.
Filing System	Means any structured set of information which is accessible according to specific criteria.
Information Officer	The Information Officer is responsible for ensuring the organisation's compliance with PAIA and POPIA. The SMG Information Officer is the Chairman of the trustees. The Deputy Information Officer responsible for management of the Security System, including the personal information collected and compliance with this policy, is the SMG Security Manager (Ashley Morkel).
Operator	An operator means a person or organisation who processes personal information for a responsible party in terms of a contract or mandate. In this case ANGOR, SMG's Managing Agent, is an operator.
Person	Means a natural or juristic person.
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).
Processing	This includes any activity or any set of activities, whether manual or automatic, on the personal information. This includes collecting, recording, organising, storing, updating, using, transmitting, distributing, linking, and destroying such information.
Record	Means any recorded information, regardless of form or medium, including: • Writing or drawing on any material, including a book, map, plan, graph or drawing, or a label identifying an object. • Information produced, recorded or stored by means of any photographic, audio or video recorder (including a computer or other device) and any material subsequently derived from this information.
Responsible Party	The responsible party is the entity that collects and processes the personal information for a particular purpose. In this case, it is the SMG Body Corporate.

Contents

3. Overview

3.1 St Martini Gardens (the Responsible party)

St Martini Gardens (SMG) is a Sectional Title Scheme Body Corporate (BC) and conducts business as a residential Sectional Title Scheme.

It acts in terms of the Sectional Titles Schemes Management Act 8 of 2011 (STSMA) which "provides for the establishment of bodies corporate to manage and regulate sections and common property in sectional titles schemes and for that purpose to apply rules applicable to such schemes".

The following rules apply to the scheme:

- The Prescribed Management Rules published as Annexure 1 to the Sectional Titles Schemes Management Regulations issued in October 2016.
- Additional Management Rules lodged with the Deeds Office in 2002.
- Conduct Rules approved by the members of the Body Corporate (BC) and CSOS[1].

The functions and powers of the BC are performed and exercised, in terms of the STSMA and the rules, by the trustees of the BC holding office. The trustees of the BC are elected at each Annual General Meeting.

3.2 Scheme Management

3.2.1 The BC has contracted the services of ANGOR Property Specialists (Pty) Ltd (ANGOR) as Managing Agent. They act on the instructions of the BC (represented by the trustees) in line with a Scope of Work which includes the following:

- Assist the BC with compliance with legislation and contractual matters.
- Provide Secretarial support.
- Provide Financial management, including budgeting, accounting, collection of levies and other monies due, payments to service providers and employees, insurance policies, bank accounts, and tax matters.
- Provide Administrative management, including the keeping of member records and correspondence, and management of service provider and employee contracts.

This includes recording and processing personal information on members (owners), employees and service providers as an **Operator.**

3.2.2 The BC employs a Building Manager and a Security Manager who act on the instructions of the BC (represented by the trustees) in line with their employment contracts, in order to provide Physical management of the scheme, including security and access control. This includes recording and processing personal information on residents, visitors, employees, service providers and others who access the premises.

[1] Approved by members on 30th November 2020 and by CSOS on 5th March 2021

4. Conditions for lawful processing of personal information

4.1 Accountability

4.1.1 Failure to comply with POPIA may damage the BC's reputation or expose the BC to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.

4.1.2 Specific responsibilities for SMG information are described in **6. SMG responsibilities**.

4.2 Processing limitation

4.2.1 The BC will ensure that personal information under its control is collected and processed:

- in a fair, lawful and non-excessive manner, and
- only for a specifically defined purpose.

4.2.2 The BC will not distribute or share personal information with any individuals or organisations that are not directly involved with the purpose for which the information was originally collected.

4.2.3 Records will be destroyed once they no longer serve the purpose for which they were collected, unless subject to a statutory retention period.

4.3 Purpose specification

4.3.1 The BC will process personal information only for specific, explicitly defined and legitimate reasons, described in **5.1 Purpose of collecting personal information**.

4.4 Further processing limitation

4.4.1 Where the BC seeks to process any personal information it holds for a purpose other than the original purpose for which it was collected the BC will obtain additional consent from the data subject (**5.4 Data subjects' rights**)..

4.5 Information quality

4.5.1 The BC will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading. The data subject has the right to check and correct their information (**5.4 Data subjects' rights**).

4.6 Openness

4.6.1 The BC will take reasonable steps to notify data subjects that their personal information is being collected, including the purpose for which it is being collected and processed. Notices are posted at all entrances to the site indicating that the premises are monitored by CCTV, and Access Registers include a privacy statement.

4.6.2 This policy document will be made available on the SMG Website stmartinigardens.co.za.

4.7 Security safeguards

4.7.1 The BC will manage the security of its information systems to ensure that personal information is adequately protected **(7. Information Security Measures**).

4.8 Data subject participation

4.8.1 Data subjects who want to make enquires about the policies and/ or their personal information, or to report an alleged infringement of their rights may contact the Information Officer (**5.4 Data subjects' rights**).

5. Processing of personal information

5.1 Purpose of collecting personal information

5.1.1 The BC collects and processes personal information in order to:

- Comply with the Sectional Titles Schemes Management Act 8 of 2011 (STSMA), particularly Management Rules 26 and 27.
- Comply with other legislation.
- Protect the physical safety and security of the scheme's residents and owners and their property, in terms of the SMG Conduct Rules and the SMG Security Information Policy.
- Communicate with owners and residents on matters relating to community living, in terms of the SMG Management and Conduct Rules.

5.1.2 Personal information will only be used for other purposes:

- When consent has been obtained from the data subject,
- When there is a legitimate and lawful reason;
- When it is required in terms of law to ensure the proper functioning of the Scheme

5.2 Personal information held by SMG

5.2.1 The personal information held by and on behalf of SMG includes (but is not limited to):

- Lists of trustees, members and tenants with full names; identity numbers or, in the case of non-South African citizens, their passport numbers; and section addresses and mailing addresses, if different; telephone numbers; and email or other electronic addresses, if any.
- Lists of registered bondholders.
- Minutes of general and trustee meetings.
- Books of account that record all its income, expenditure, assets and liabilities; disclose all amounts recovered from members by the body corporate or any managing agent or other service provider acting on its behalf; including individual accounts for each member.
- Names, addresses, identity numbers and contact details of employees.
- Names, addresses and contact details of service providers.
- CCTV recordings, access control system records and access registers of persons on site.
- Resident names and contact numbers in the wireless intercom system
- On-site security Occurrence Book and supporting information.
- Correspondence between the trustees, and with the managing agent, members and residents and others;
- Correspondence between the Building manager and the Security manager, and with the trustees, managing agent, members, residents, service providers and others;
- Correspondence between employees of the managing agent, and with trustees, members, residents, service providers and others.

5.2.2 To comply with the regulations currently in place in terms of the Disaster Management Act (57 of 2002) and the SMG COVID-19 Workplace Compliance Plan, a register of employees, BC contractors and members' contractors entering the site is completed including the subjects' temperatures. This is **Special Personal Information**. The use and release of this information is managed in terms of the SMG Security Information Manual.

5.2.3 The on-site records (CCTV recordings, access control system records and access registers) may include **personal information of persons under 18.**
The use and release of this information is managed in terms of the SMG Security Information Manual.

5.2.4 There is no trans-border flow of personal information except to owners who live overseas, in terms of STSMA PMR 27.

5.3 Data subjects

A data subject is the natural or juristic person to whom personal information relates. This includes:

5.3.1 Members (owners);

5.3.2 Residents (owners, tenants and others);

5.3.3 Residents' visitors (including employees and service providers);

5.3.4 BC employees and service providers.

5.4 Data subjects' rights

5.4.1 A data subject has the right to establish whether the organisation holds personal information related to him/her, to inspect their personal information held by the organisation, and to correct it.

5.4.2 A data subject may object to the processing of his/her personal information and request deletion of this information. Unless this is subject to any statutory and contractual record keeping requirements, the organisation must comply.

5.4.3 A data subject has the right to object to the processing of his/her personal information for any purpose other than the purpose(s) for which it was collected.

5.4.4 A data subject has the right to be notified that his/her personal information is being collected by the organisation, and 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.

5.4.5 A data subject has the right to appeal to the Information Officer regarding an alleged infringement of any of the rights protected under POPIA.
If the matter is not resolved internally, s/he may submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and/ or to institute civil proceedings in a relevant court regarding the alleged non-compliance with the protection of his/her personal information.

5.5 Collection of personal information

5.5.1 Personal Information is collected directly from the data subject where possible.

5.5.2 Notices are posted at all entrances to the site indicating that the premises are monitored by CCTV: CCTV recordings and access control system records are considered to be collected directly from the data subject.

5.6 Use and distribution of personal information

5.6.1 Personal information will only be used or distributed:

- When consent has been obtained from the data subject,
- When there is a legitimate and lawful reason;
- When it is required in terms of law to ensure the proper functioning of the Scheme

5.6.2 Access to personal information may be requested in terms of the SMG PAIA Manual.

5.6.3 In terms of the STSMA, information is sent to members, registered bondholders and persons authorised in writing by a member or registered bondholder from time to time. This includes (but is not limited to) minutes of member and trustee meetings, and reports circulated to members before General Meetings. This may include personal information. A privacy statement along the following lines should appear on all such documents:

The Body Corporate of St Martini Gardens undertakes to take reasonable steps to protect the confidentiality and security of personal information. Personal information in this document is disclosed in terms of STSMA Prescribed Management Rules 26 & 27 to members, registered bondholders and persons authorised in writing by a member or registered bondholder. This information should not be distributed further, or used for any other purpose.

5.7 Retention of personal information records

5.7.1 Records held in terms of the STSMA:

- Meeting minutes and scheme details are retained for the lifetime of the scheme.
- Trustee, member, tenant and bondholder records are retained for five years after the person ceases to be a trustee, member, tenant or bondholder.
- Financial records are retained for six years after completion of the transactions to which they relate.

5.7.2 Records held in terms of the SMG Security Information Policy:

- CCTV records are automatically overwritten, usually after two to three weeks.
- Access tag records are normally deleted two months after the tag-holder moves out.
- Unless required for ongoing investigations, Whatsapp messages are deleted after one week.
- Occurrence Books, Incident Reports and Access Registers are shredded after five years.
- Wireless intercom system data is deleted when the resident moves out, or on the request of the data subject.
- COVID-19 screening registers are kept for four weeks.
- Copies of records made in the course of investigations by the BC will be destroyed after 180 days, unless otherwise requested in writing for a valid purpose, in which case they will be destroyed as soon as the purpose is achieved.

5.7.3 Records held in terms of other legislation will be retained in line with that legislation, or for five years.

5.8 Deletion of personal information records

5.8.1 Destruction of paper records will be by shredding.

5.8.2 Deletion of electronic records will be assured, to ensure that deleted information is incapable of being reconstructed or recovered.

6. SMG responsibilities

6.1 Body Corporate

6.1.1 The BC is ultimately accountable for ensuring that it meets its legal obligations in terms of POPIA.

6.1.2 The functions and powers of the BC are performed and exercised, in terms of the STSMA and the rules, by the trustees of the BC holding office and elected at each Annual General Meeting.

6.1.3 Some of the BC's responsibilities in terms of POPIA are delegated to employees and service providers.

6.1.4 The BC is responsible for appointing an Information Officer, and (where considered necessary) Deputy Information Officers, and ensuring that they are registered with the South African Information Regulator.

6.1.5 The following people are responsible for the BC's information:

Responsibility	Name	Position
Information Officer	Glyn Fogell	Trustee Chairman Trustee responsible for information technology and security matters
Deputy Information Officers	Riedewaan Abdullah	Building Manager
	Ashley Morkel	Security Manager
	Marion Fogell	Trustee responsible for governance

They may all be contacted at the BC's physical/ service address.

6.2 Information Officer

The Information Officer, assisted by the Deputy Information Officers, is responsible for ensuring that:

6.2.1 Policies relating to access to and protection of the BC's information are developed and maintained in line with STSMA, POPIA, PAIA and other legislation.

6.2.2 All persons responsible for the processing of personal information on behalf of the BC are:

- Fully aware of the risks associated with the processing of personal information;
- Informed about the BCs' security controls, and appropriately trained and supervised to do so;
- Contractually obligated to protect the personal information they come into contact with; and
- Aware that a wilful or negligent breach of the BC's policies and procedures may lead to disciplinary and/ or legal action being taken against them.

6.2.3 Data subjects who want to make enquires about the policies and/ or their personal information are enabled to do so.

6.2.4 Protection of personal information statements and disclaimers are displayed on BC communications that may include personal information.

6.2.5 Security breaches are disclosed and reported to the Body corporate and the Information Regulator, as required.

6.2.6 The BC's information technology infrastructure, filing systems and all devices used for processing personal information meet acceptable security standards.

6.2.7 A periodic Privacy Review is held, in order to assess and review the ways in which the BC collects, holds, uses, shares, discloses, destroys and processes personal information.

6.2.8 Cooperation is given to the Information Regulator in relation to any information-related matters, including ongoing investigations.

6.3 Trustees

In order to perform their duties the SMG trustees have access to all the scheme's personal information.

This information is protected in terms of this Privacy Policy, and in terms of Section 8(1) of the STSMA "trustees stand in a fiduciary relationship to the BC" and 8(2)(a)". must in relation to the body corporate act honestly and in good faith, and in particular (i) exercise his or her powers in terms of this Act in the interest and for the benefit of the body corporate; and (ii) not act without or exceed those powers".

6.4 Managing Agent

6.4.1 In order to perform their duties **ANGOR** collects, processes and files SMG's governance and financial information. This includes personal information of members, employees and service providers. This is collected and processed in terms of Prescribed Management Rule 27 of the STSMA.

6.5 Employees & contractors

6.5.1 In order to perform their duties the **Building and Security Managers** collect, process and file personal information relating to those on site, especially residents, employees, visitors and service providers.

- Resident information is collected and processed by the Building Manager in terms of Prescribed Management Rule 27 of the STSMA.
- Employee information is collected and processed by the Building Manager to meet operational needs, and in terms of labour legislation.
- Information relating to persons on site, especially residents, visitors and service providers, is collected and processed in terms of SMG rules and processes.

  This information is protected in terms of this Privacy Policy, the SMG Security Information Manual and signed confidentiality agreements attached to each of their employment contracts.

6.5.2 In order to perform their duties the **on-site Security Officers** have custody of some of SMG's personal information relating to those on site, especially residents, visitors and contractors.

This information is protected in terms of this Privacy Policy; a confidentiality clause is included in the signed SMG Security Procedures Manual (Scope of Work) and confidentiality agreements are included in their employment contracts.

6.5.3 In the performance of their duties the **on-site cleaning staff** may become aware of personal information relating to those on site, especially residents, visitors and contractors.
This information is protected in terms of a confidentiality clause included in the Service Provider's Service Agreement and confidentiality agreements that are included in their employment contracts.

7. Information Security Measures

7.1 ANGOR

7.1.1 SMG's governance and financial information held by ANGOR is protected in terms of the Management Agreement dated 10 November 2021 and their Privacy Policy (on their website).

7.2 On-site written information

7.2.1 Written records held on-site at SMG that may include personal information include:

- Lists of residents and owners.
- Quotes, invoices and statements from service providers.
- Employee records.
- Access registers.
- Printouts of digital records.
- On-site security Occurrence Book and supporting information.
- Written correspondence between the Building Manager and the Security Manager with the trustees, managing agent, members, residents, service providers and others.

7.2.2 Access registers and Occurrence books currently in use are kept in the security cubicles, in the custody of the officer on duty.

7.2.3 All personal information will be filed appropriately, and when unattended will be kept in a locked cupboard in a locked room.

7.2.4 Keys will only be made available to authorised persons.

7.3 On-site digital information

7.3.1 Digital information (on computers) held on-site at SMG that may include personal information include:

- Lists of residents and owners.
- Quotes, invoices and statements from service providers.
- Employee records,
- Minutes of meetings.
- CCTV recordings.
- Access control system records.
- Resident names and contact numbers in the wireless intercom system.
- E-mail correspondence between the Building manager and the Security manager with the trustees, managing agent, members, residents, service providers and others.

7.3.2 E-mails containing personal information are marked as Confidential, and only sent to those entitled to such information.

7.3.3 All computers that may hold personal information are protected with a userid and password, and when unattended will be locked inside a locked room.

7.3.4 Passwords and keys will be protected, and only made available to authorised persons.

7.4 Computer system security

7.4.1 The BC's personal computers and other devices used for processing personal information meet acceptable security standards. This includes:

- Computers containing personal information are sited in secure locations (locked offices).
- All digital information is backed-up and tested on a regular basis.
- All back-ups containing personal information are protected from unauthorised access and accidental deletion.
- Computers containing personal information are protected by security software including up-to-date anti-virus software and a firewall.
- Service providers supporting the BC's digital services and information are required to sign confidentiality agreements and/or submit acceptable privacy policies to ensure the protection of SMG's personal information.
- Regular Reviews are performed to ensure that the security of the Body Corporate's hardware and software systems are functioning properly.

7.5 Privacy reviews

7.5.1 The BC's Information Officer will schedule periodic Privacy Reviews in order to:

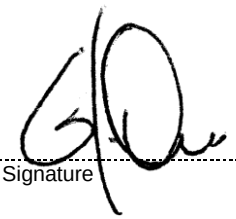
- Identify the processes used to collect, record, store, disseminate and destroy personal information.
- Determine the flow of personal information throughout the BC.
- Redefine the purpose for gathering and processing personal information.
- Ensure that the processing parameters are still adequately limited.
- Ensure that new data subjects are made aware of the processing of their personal information.
- Re-establish the rationale for any further processing where information is received via a third party.
- Verify the quality and security of personal information.
- Monitor the extend of compliance with POPIA and this policy.
- Monitor the effectiveness of internal controls established to manage the Body Corporates' POPI related compliance risk.

7.5.2 In performing the Privacy Review the Information Officer will liaise with the Deputy IOs, trustees, employees and service providers in order to identify areas within the BC's operation that are most vulnerable or susceptible to the unlawful processing of personal information.

7.5.3 zA summary of the findings from the Privacy Review will be included in the annual Trustee Report to members.

8. Approval

Glyn Fogell
Information Officer



Signature

31/01/2022

Date

Glossary of acronyms

BC	Body Corporate
IO	Information Officer
PAIA	Promotion of Access to Information Act, 2000
POPIA	Protection of Personal Information Act, 2013
SMG	St Martini Gardens
STSMA	Sectional Titles Schemes Management Act, 2011
ANGOR	ANGOR Property Specialists (Pty) Ltd