

**PROTECTION OF PERSONAL INFORMATION (POPI)
POLICY OF**

THE ISLANDS HOMEOWNERS ASSOCIATION NPC

Registration Number: 2006/038143/08

("the Company")

**prepared in accordance with the provisions of the Protection
of Personal Information Act 4 of 2013 ("POPIA")**

THE ISLANDS HOMEOWNERS ASSOCIATION
NPC Registration Number 2006/038143/08



TABLE OF CONTENTS

| | |
|---|----|
| 1. INTRODUCTION | 3 |
| 2. INTERPRETATION & DEFINITIONS | 3 |
| 3. COLLECTION OF PERSONAL INFORMATION | 5 |
| 4. PURPOSE, PRINCIPLES, SCOPE & FRAMEWORK OF POLICY | 6 |
| 4.1 SCOPE OF THIS POLICY | 6 |
| 4.2 PURPOSE OF THIS POLICY | 6 |
| 4.3 PRINCIPLES OF THIS POLICY | 7 |
| 5. KEY OPERATIONAL FRAMEWORK | 7 |
| 6. THE INFORMATION OFFICER | 8 |
| 7. SECURITY OF DATA - RETENTION AND DISPOSAL | 9 |
| 8. CLOSED-CIRCUIT TELEVISION (CCTV) | 10 |
| 9. WEBSITE | 11 |
| 9.1 COLLECTION OF NON-PERSONAL INFORMATION | 11 |
| 9.2 "COOKIES" POLICY | 11 |

Copyright subsists in this work. No part of this work may be reproduced in any form or by any means without the author's written permission. Any unauthorized reproduction of this work will constitute a copyright infringement and render the doer liable under both civil and criminal law. A.C. Rooseboom t/a Rooseboom Attorneys ("Rooseboom Attorneys") owns the copyright of this material. Rooseboom Attorneys grants license to use any material by **the Company** only, and any future use for entities or individuals, other than **the Company**, shall be in breach of the copyright held subsisting in this work.

1. INTRODUCTION

- 1.1 We respect the privacy of everyone who resides in or owns property in the Company. As a result, we would like to inform you regarding the way we would use your Personal Information. We recommend you read this Policy so that you understand our approach towards the use of your Personal Information.
- 1.2 This Policy explains how we obtain, use and dispose of your Personal Information, as is required by the Protection of Personal Information Act No. 4 of 2013 (POPI Act). We are committed to protecting your privacy impact and to ensure that your Personal Information is collected and used properly, lawfully, and openly.

2. INTERPRETATION & DEFINITIONS

- 2.1 In this Policy, unless the context otherwise indicates:
- 2.1.1. the singular shall import and include the plural and *vice versa*; and
- 2.1.2. words indicating one gender shall import and include the other gender; and
- 2.1.3. words indicating natural persons shall import and include artificial persons; and
- 2.1.4. the head notes or clause headings to this Policy are used for the sake of convenience only and shall not govern the interpretation of the clause to which they relate; and
- 2.1.5. the following words and expressions shall, in addition to their respective ordinary meanings, bear the following meanings assigned to each of them respectively:
- 2.1.5.1. **“Company”** means **The Islands Homeowners Association NPC** (Reg No: 2006/038143/08), a company duly registered and incorporated in accordance with the Company Laws of the Republic of South Africa and having its principal place of business situated at R512 Provincial Road, Broederstroom, North West Province, Republic of South Africa; and
- 2.1.5.2. **“Conditions for Lawful Processing”** means the conditions for the lawful processing of Personal Information as fully set out in Chapter 3 of POPIA; and
- 2.1.5.3. **“Constitution”** means the Constitution of the Republic of South Africa, 1996; and
- 2.1.5.4. **“Data Subject”** has the meaning ascribed thereto in Section 1 of POPIA; and
- 2.1.5.5. **“Estate”** means Access Erven, Common Property Erven and other Company Erven and situated at R512 Provincial Road, Broederstroom, North West Province, Republic of South Africa; and
- 2.1.5.6. **“Head of the Company”** means the “head” as defined in Section 1 of PAIA; and
- 2.1.5.7. **“Information Officer”** means Information Officer and Director of the Company so appointed, as referred to in POPIA; and
- 2.1.5.8. **“Member”** means a registered owner / s of an Erf or as defined in the

Alienation of Land Act No. 68 of 1981 and who is, as a result of such ownership, a member of the Company; and

- 2.1.5.9. “**PAIA**” means the *Promotion of Access to Information Act No. 2 of 2000*; and
- 2.1.5.10. “**Personal Information**” has the meaning ascribed thereto in Section 1 of POPIA; and
- 2.1.5.11. “**Personnel**” refers to any person who works for, or provides services to or on behalf of the Company, and receives or is entitled to receive remuneration and any other person who assists in carrying out or conducting the business of the Company, which includes, without limitation, all directors / all directors, all permanent, temporary and part-time staff as well as contract workers; and
- 2.1.5.12. “**POPIA**” means the *Protection of Personal Information Act No. 4 of 2013*; and
- 2.1.5.13. “**POPIA Policy**” means such Policy as adopted by the Company in compliance with the provisions of POPIA, and as amended from time to time; and
- 2.1.5.14. “**POPIA Regulations**” mean the regulations promulgated in terms of Section 112(2) of POPIA; and
- 2.1.5.15. “**Private Body**” has the meaning ascribed thereto in Sections 1 of both PAIA and POPIA; and
- 2.1.5.16. “**Processing**” has the meaning ascribed thereto in Section 1 of POPIA; and
- 2.1.5.17. “**Regulator**” means the Information Regulator established in terms of Section 39 of POPIA; and
- 2.1.5.18. “**Responsible Party**” has the meaning ascribed thereto in Section 1 of POPIA; and
- 2.1.5.19. “**Record**” has the meaning ascribed thereto in Section 1 of PAIA and includes Personal Information; and
- 2.1.5.20. “**Requester**” has the meaning ascribed thereto in Section 1 of PAIA; and
- 2.1.5.21. “**Request for Access**” has the meaning ascribed thereto in Section 1 of PAIA; and
- 2.1.5.22. “**Sensitive Personal data**” – includes the following:
- Racial or ethnic origin;
 - Political opinions;
 - Religious or similar beliefs;
 - Financial Information;
 - Mental or physical health;
 - Family details;
 - Criminal records or allegations of criminal conduct.

2.1.5.23. “SAHRC” means the South African Human Rights Commission.

- 2.2. Capitalised terms used in this Policy have the meanings ascribed thereto in Section 1 of POPIA and PAIA as the context specifically requires, unless otherwise defined herein; and
- 2.3. Where any other term is defined within the context of any particular clause in this Policy (other than definitions appearing in clause 1), unless it is clear from the clause in question that the term so defined has application to the entire Policy, that defined term shall bear the meaning ascribed to it for the entire main parent clause wherein it is defined (i.e. clause 1 or 2 or 3 etc), including all sub-clauses thereto, and not for the entire Policy; and
- 2.4. When any number of days is prescribed in this Policy, same shall be reckoned exclusively of the first and inclusively of the last day, unless the last day falls on a Saturday, Sunday or public holiday, in which case, the last day shall be the next succeeding day which is not a Saturday, Sunday, or public holiday. The term “business day” shall mean any day other than a Saturday, Sunday or public holiday; and
- 2.5. Annexures to this Policy that do not themselves contain their own definitions expressions defined in this Policy shall bear the same meanings in such annexures; and
- 2.6. The use of the word “including” followed by a specific example/s shall not be construed as limiting the meaning of the general wording preceding it and the *eiusdem generis* (of the same type) rule shall not be applied in the interpretation of such general wording or such specific example/s; and
- 2.7. This Policy and all matters or disputes arising therefrom or incidental thereto, shall be governed and construed in accordance with the laws of the Republic of South Africa.

3. COLLECTION OF PERSONAL INFORMATION

- 3.1 We collect and Process your Personal Information mainly to provide you with access to the Company, to help us improve our offerings to you, in order to exchange correspondence and or account statements to you and to support our relationship with you and for certain other purposes explained below. The type of information we collect will depend on the purpose for which it is collected and used. We will only collect information that we need for that purpose.
- 3.2 We collect Personal Information directly from you where you provide us with your personal details, for example when you are a Member / resident, and when you submit enquiries to us or contact us. Where possible, we will inform you what information you are required to provide to us and what information is optional.
- 3.3 Examples of Personal Information we collect from you are:
- a) name
 - b) address
 - c) email address
 - d) telephone/cell number
- 3.4 Access to Personal Information will be and can be given to:
- a) Auditors and / or Accountants of the Company; and
 - b) Attorneys and / or Counsel appointed by the Company; and
 - c) Managing Agents and their Personnel; and
 - d.) Owners (certain Owner sensitive information will not be disclosed and will require a formal PAIA application to be submitted and adjudicated on).

4. PURPOSE, PRINCIPLES, SCOPE & FRAMEWORK OF POLICY

4.1 SCOPE OF THIS POLICY

Personal Information may only be processed if, given the purpose for which is processed is:

- a) Adequate; and
- b) Relevant; and
- c) Not excessive

| | OWNERS / MEMBERS | TENANTS | DIRECTORS | VISITORS | STAFF / WORKERS |
|---|---|---|---|---|---|
| How Personal Information is collected | <ul style="list-style-type: none"> • Public Records • Owner | As required in terms of Law | From Directors | From Visitors | From Staff / Workers |
| What Personal Information is collected | <ul style="list-style-type: none"> • Full Names • Identity Numbers • OR Passport Numbers • Section and Mailing Addresses • Telephone Numbers • E-mail or other Electronic Addresses | <ul style="list-style-type: none"> • Full Names • Identity Numbers • OR Passport Numbers • Section and Mailing Addresses • Telephone Numbers • E-mail or other Electronic Addresses | <ul style="list-style-type: none"> • Full Names • Identity Numbers • OR Passport Numbers • Section and Mailing Addresses • Telephone Numbers • E-mail or other Electronic Addresses | <ul style="list-style-type: none"> • Full Names; • Identity Numbers • Or Passport Numbers; • Driver's License | <ul style="list-style-type: none"> • Full Names; • Identity Numbers, • OR Passport Numbers; • Mailing Addresses |
| How Personal Information is held | <ul style="list-style-type: none"> • Hard copy • Electronically | <ul style="list-style-type: none"> • Hard copy • Electronically | <ul style="list-style-type: none"> • Hard copy • Electronically | <ul style="list-style-type: none"> • Hard copy • Electronically | <ul style="list-style-type: none"> • Hard copy • Electronically |
| Purpose of holding Personal Information | <ul style="list-style-type: none"> • Comply with Legislation • Communication | <ul style="list-style-type: none"> • Comply with Legislation • Communication | <ul style="list-style-type: none"> • Comply with Legislation • Communication | Safety | Communication |
| Access to Personal Information | As Required in terms of Law | As Required in terms of Law | As Required in terms of Law | Consent Required | Consent Required |

4.2 PURPOSE OF THIS POLICY

The purpose of this Policy is to enable the Company to:

- a) Comply with relevant legislation in respect of Personal Information it processes / retains about Personnel / Staff, directors, Visitors, Members and contractors / service providers; and
- b) To follow good practice and to protect Personnel / Staff, directors, Visitors and Members; and
- c) To respect individual's rights; and
- d) To ensure that any Personal Information held is not being misused; and
- e) To protect the Company from the consequences of a breach of its responsibilities.

4.3 **PRINCIPLES OF THIS POLICY**

- 4.3.1 This Policy applies to all Personnel / Staff, directors, Visitors, Members, and contractors / service providers assigned to / contracted to the Company.
- 4.3.2 Personnel must be informed about data protection issues, and their rights to access their own Personal Information through the induction process. All directors will receive guidance on data protection during their induction and any contractors should be briefed on the importance of data protection at the start of their assignment, as it relates to safeguarding sensitive Personal Information on a Member, resident, contractor, or guest.
- 4.3.3 All Personnel of the Company will be required to sign an addendum to their employment contracts containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPIA.
- 4.3.4 Compliance with this Policy is a condition of appointment with the Company and any breach of the Policy may result in disciplinary action, which for serious or deliberate breaches may include dismissal. Knowingly breaching the provisions of POPIA and PAIA may also lead to legal action being taken against the organization and individuals in breach.
- 4.3.5 All product suppliers, insurers and other third-party service providers will be required to sign a service level agreement guaranteeing their commitment to the Protection of Personal Information; this is however an ongoing process that will be evaluated as needed.
- 4.3.6 All data/information processed by the Company is covered by this Policy.

5. **KEY OPERATIONAL FRAMEWORK**

- 5.1 Processing of Personal Information will only be carried out where the Data Subject has given consent. This includes implied consent, for example where the data is necessary for the performance of:
- 5.1.1 a contract to which the Data Subjects are a party; or
- 5.1.2 for taking steps at the request of the Data Subject with a view to entering a contract of employment or other legal obligation such as operational services or personal support services; or
- 5.1.3 the processing is necessary for performing any obligation imposed by law on the Company in connection with offers of tenancy, service, or employment; or
- 5.1.4 the processing is necessary to protect the operation of services and vital interests of the Data Subject or another person in a case where:
- a) consent cannot be given by the individual.
 - b) the Company and / or its directors cannot be reasonably expected to obtain the consent; or
 - c) in order to protect the vital interests of another person in a case where the consent by or on behalf of the Data Subject has been unreasonably withheld. Details of the reasons why the data is sought and the reasons

for which it will be used will be stated on all relevant forms as outlined in the Appendix hereto containing a schedule of all the forms in terms of POPIA.

5.2 We will use your Personal and Non-Personal Information only for the purposes for which it was collected or agreed with you, for example:

- a) Access control and CCTV data.
- b) Residents and Members database.
- c) Official communication through e-mail or Push Notifications.
- d) For audit and record keeping purposes.
- e) For monitoring and auditing site usage.
- f) In connection with any legal proceedings.
- g) To carry out obligations arising from any contracts entered between you and us.
- h) To confirm and verify your identity or to verify that you are an authorised visitor for security purposes.
- i) To respond to your queries or comments.
- j) We may also use your Personal Information to comply with legal and regulatory requirements or industry codes to which we subscribe, or which apply to us, or when it is otherwise allowed by law.

5.3 You have the right to ask us to update, correct or delete your Personal Information. We will take all reasonable steps to confirm your identity before making changes to Personal Information we may hold about you. We would appreciate it if you would take the necessary steps to keep your Personal Information accurate and up to date by immediately notifying us in writing of any changes, we need to be aware of.

5.4 The processing of Sensitive Personal Data will only be carried out with the Data Subject's express consent. In the event of the Data Subject being a minor, the express consent from the parent / guardian shall be obtained.

5.5 Personal Information received from third parties, which included Personal Information which has been provided to the directors or Managing Agent of the Company in confidence, by a third party such as employment references or tenancy reports, cannot normally be disclosed to the Data Subject, unless the author of the Personal Information (third party) can remain anonymous, agrees to its release at a later date or it is reasonable to comply with the access request without the originator's consent.

5.6 Where Personal Information is held by the Company on residents, owners, tenants, applicants, Personnel and other individuals, these people have the right to access the information, unless it is exempt under the POPIA and PAIA.

6. THE INFORMATION OFFICER

6.1 The Company will appoint a responsible person to process Personal Information (the "Information Officer"). The Information Officer's details will be announced from time-to-time. Consideration will be given on an annual basis of the re-appointment or replacement of the Information Officer as well as the need to appoint and / or replace a Deputy Information officer as stipulated per POPIA.

6.2 The Information Officer shall have the following responsibilities:

- a) Ensure compliance with the Policy and POPIA.
- b) Review this Policy periodically.
- c) Ensure that all Personal Information processed is always secured and kept confidential, save as where disclosure is required in terms of the Law.

- d) Ensure all contracts contain a clause regarding POPIA compliance.
- e) Ensure that all Personal Information is accurate, complete, and up to date.
- f) Ensure Personal Information is processed correctly in terms of this Policy.
- g) Ensure correctness and completeness of Personal Information.
- h) Ensure all Personal Information is kept safely and securely.
- i) Always ensuring adequate safeguards in place.
- j) Handle requests for access to Personal Information.
- k) Provide access to Personal Information when required to do so in terms of applicable legislation.
- l) Ensure Personal Information is destroyed when required.
- m) Safekeeping of PAIA Manual.
- n) Assist the Information Regulator in respect of any investigation.
- o) Handling all aspects of relationship with the Regulator.
- p) Notify persons as well as Regulator immediately in the event of a breach.

7. SECURITY OF DATA - RETENTION AND DISPOSAL

- 7.1 All Personnel are responsible for ensuring that any Personal Information which they hold is kept securely and that they are not disclosed to any unauthorized third party.
- 7.2 All Personal Information must be accessible only to those who need to use it. A judgment made by the Information Officer when considering the granting of access to Personal Information should be based upon the sensitivity and value of the information in question; but always consider keeping Personal Information:
- 7.2.1 in a lockable room with controlled access; and
 - 7.2.2 in a locked drawer or filing cabinet; and
 - 7.2.3 if Personal Information is computerized then it should be stored on network servers and not on local systems and have suitable security access levels applied; and
 - 7.2.4 particular care should be taken of portable computer equipment, memory sticks etc. which should be password protected to prevent unauthorized access. Where Personal Information is by necessity stored on memory sticks these must be protected by advanced encryption and passwords strictly controlled by the Information Officer and / or Deputy Information Officer / s; and
 - 7.2.5 sensitive Personal Information should never be kept on memory sticks or routinely taken from the Company or Managing Agent premises on any form of removable media; and
 - 7.2.6 Personal Information held on removable media such as CD/DVD media must be disposed of in accordance with acceptable information / data disposal methods.
- 7.3 Care must be taken to ensure that computer monitors, and mobile device screens are not visible except to authorized Personnel and that computer passwords are kept strictly confidential. Computers, mobile phones, Notebooks, and laptops should not be left unattended without password protected screen savers; manual records should not be left where they can be accessed by unauthorized Personnel. Personnel and employees are encouraged to operate a “clear desk” policy when finishing work each day.
- 7.4 Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of Personal Information. Manual records should be shredded or disposed of as “confidential waste”.

- 7.5 This Policy also applies to Personnel and / or directors and / or employees of the Managing Agent who process Personal Information outside the Company premises, such as when working from home. Off-site processing presents a potentially greater risk of loss, theft, damage to Personal Information. Personnel should take particular care when processing Personal Information at home or in other locations. Any loss / breach of Information from either the Company premises or off site must be reported to the Information Officer immediately.
- 7.6 The directors of the Company discourage the retention of Personal Information for any longer than necessary. Personal Information shall not be kept for longer than is necessary for that purpose. Considerable amounts of Personal Information are collected, and some Personal Information will be kept for longer periods than others, however every effort should be made to review the need to keep it and safely dispose thereof as soon as possible.
- 7.7 The Company shall retain Personal Information according to the following guidelines (which may be revised as from time to time):
- 7.7.1 Personal Information regarding members and occupants shall be retained for a period of 5 (five) - 10 (ten) years after the person is no longer a member or occupant of the Company, whereafter, that information which is not in the public domain is to be destroyed; and
 - 7.7.2 Any Personal Information contained in the Company's books of account shall be retained for a period of 6 (six) years; and
 - 7.7.3 Visitors' private information shall be retained for a period of 3 (three) years whereafter, same will be destroyed.
 - 7.7.4 Personal Information of Personnel shall be retained for a period of 5 (five) - 10 (ten) years after the Personnel / staff is no longer employed by the Company, whereafter, that information which is not in the public domain is to be destroyed; and
 - 7.7.5 Director's information will be kept indefinitely.
- 7.8 Personal Information will be disposed of in a way that protects the rights and privacy of Data Subjects (e.g. shredding, disposal as confidential waste, deletion from ICT systems and backups).

8. CLOSED-CIRCUIT TELEVISION (CCTV)

- 8.1 The Company has a requirement for maintaining security using Closed-Circuit Television Systems. (hereinafter referred to as "CCTV")
- 8.2 The use of CCTV must be authorized and utilized in compliance with POPIA, and do not require the consent of owners, residents, visitors, contractors / service providers, and Personnel.
- 8.3 Where CCTV is used, images are treated as Personal Information in the same manner as paper or computer-based information. The main purpose of collecting Personal Information in the form of camera recordings from CCTV cameras is the protection of all tenants, residents, contractors / service providers, visitors / guests, employees and the public, the prevention of crime or anti-social behavior and to safeguard the common property of the Company. All stored recordings / data from CCTV cameras may be used as evidence during criminal or other legal proceedings. CCTV shall not be used to monitor private areas such as inside a home or garden.

- 8.4 CCTV Systems in use by the Company are monitored on a constant basis. Personnel check the systems constantly. Personnel should not use the system for monitoring movements of people outside the boundaries of the common property. Personnel are not to be expected to respond to requests from other residents who, for example, may want to find out what time and whereabouts of someone's movements are or were.
- 8.5 Images will be recorded on a time loop. This means that recorded images are not kept indefinitely and will be recorded over on a regular basis. The length of time images is stored before being overwritten is known to Personnel responsible for monitoring the system to respond to enquiries from authorized parties.
- 8.6 Recorded images are kept securely, and Personnel may not access these without the permission of the Information Officer and only for specific purposes related to the use of CCTV, i.e., crime prevention/detection or dealing with anti-social behavior.
- 8.7 CCTV images are the property of the Company.

9. WEBSITE

9.1 COLLECTION OF NON-PERSONAL INFORMATION

We may automatically collect non-Personal Information about you, such as the type of internet browsers you use or the website from which you linked to our website. We may also aggregate details which you have submitted to the site (for example, the products or services you are interested in). You cannot be identified from this information and it is only used to assist us in providing an effective service on this web site. We may from time to time supply third parties with this non-personal or aggregated data for uses in connection with this website.

9.2 "COOKIES" POLICY

We use the term "cookies" to refer to cookies and other similar technologies covered by the POPIA on privacy in electronic communications.

9.2.1 What is a cookie?

Cookies are small data files that your browser places on your computer or device. Cookies help your browser navigate a website and the cookies themselves cannot collect any information stored on your computer or your files. When a server uses a web browser to read cookies, they can help a website deliver a more user-friendly service. To protect your privacy, your browser only gives a website access to the cookies it has already sent to you.

9.2.2 Why do we use cookies?

We use cookies to learn more about the way you interact with our content and help us to improve your experience when visiting our website. Cookies remember the type of browser you use and which additional browser software you have installed. They also remember your preferences, such as language and region, which remain as your default settings when you revisit the website. Cookies also allow you to rate pages and fill in comment forms. Some of the cookies we use are session cookies and only last until you close your browser, others are persistent cookies which are stored on your computer for longer.

9.2.3 **How are third-party cookies used?**

For some of the functions within our websites we use third party suppliers, for example, when you visit a page with videos embedded from or links to YouTube. These videos or links (and any other content from third party suppliers) may contain third party cookies and you may wish to consult the policies of these third-party websites for information regarding their use of cookies.

9.2.4 **How do I reject and delete cookies?**

9.2.4.1 We will not use cookies to collect Personally identifiable Information about you. However, should you wish to do so, you can choose to reject or block the cookies set by the websites of any third-party suppliers by changing your browser settings – see the Help function within your browser for further details. Please note that most browsers automatically accept cookies so if you do not wish cookies to be used you may need to actively delete or block the cookies.

9.2.4.2 You can also visit www.allaboutcookies.org for details on how to delete or reject cookies and for further information on cookies generally. For information on the use of cookies in mobile phone browsers and for details on how to reject or delete such cookies, please refer to your handset manual. Note, however, that if you reject the use of cookies you will still be able to visit our websites but some of the functions may not work correctly.