BASIC INTERNAL OFFICE POLICY

PROCESSING INFORMATION

1. INTRODUCTION

1.1. At Bahia Formosa Estates CC (t/a Sotheby's International Realty Plettenberg Bay) we are committed to processing information pursuant to the conditions set forth in the Protecting of Personal Information Act, 4 of 2013 and the Regulations. This office policy guides the office standard for processing information of our clients and potential clients but also that of our office staff and agents.

2. PERSONAL INFORMATION

2.1. **"personal information"** is data that can be used to identify a person. It is defined as "information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person." This information about a person includes, but is not limited to: Race; Gender; Sex; Pregnancy; Marital status; National / ethnic / social origin; Colour; Sexual orientation; Age; Physical or mental health; Disability; Religion / beliefs / culture; Language; Educational / medical / financial / criminal or employment history; ID number; Email address; Physical address; Telephone number; Location; Biometric information; Personal opinions, views or preferences.

2.2. **"data subject"** is a person whose personal information has been processed. To put this in context, if you hold someone's personal **data** on file, that person is a **data subject.**

2.3. **"responsible party"** means Bahia Formosa Estates CC

2.4. **"office"** means the office of Sotheby's International Realty, 25 Main Street, Summer Hill Building, Plettenberg Bay, 6600

2.5. **"system"** means the following systems, computer software or programmes used by the agency:

2.5.1. Hand Made Software

2.5.2. Hubspot

2.5.3. Outlook email

3. INFORMATION OFFICER

3.1. The designated information officer for this agency is Steven Neufeld and his/her contact details are 044 533 2529 or steve.sir@plettenbergbay.com

3.2. All employees and staff must strictly adhere to any request pursuant to the information officer's duties.

3.3. All complaints about the information officer, his/her duties or requests must be referred to the head of the branch.

3.4. Staff and employees must remain mindful of the agency's responsibility to ensure compliance with the Act, and the respective fines that may be ascribed to the agency should it not comply.

3.5. The duties of the information officer will include:

3.5.1. Ensure that a compliance framework is developed, implemented, and monitored.

3.5.2. To encourage compliance by the organization, with the conditions for the lawful processing of personal information

3.5.3. Assist and deal with any request made in terms of the Protection of Personal Information Act, 4 of 2013 (POPIA) or Promotion of Access to Information Act, 2 of 2000 (PAIA).

3.5.4. To work with the Regulator in relation to any investigations be conducted pursuant to the POPIA.

3.5.5. Ensure compliance by the organization to POPIA and PAIA

3.5.6. To conduct continuous personal information impact assessments

3.5.7. Ensure that adequate measures and standards exist to comply with the conditions for the lawful processing of personal information.

3.5.8. Conduct regular awareness sessions regarding the provisions of the Act, regulations made in terms of the Act, codes of conducts, or information obtained from the Regulator.

3.5.9. Ensure that the organization's policies and procedures for the lawful processing of information is continuously updated and relevant to the current processes within the organization.

3.5.10. Upon request of any person provide copies of the manual to that person upon payment of a fee determined from time to time by the Regulator.

3.5.11. Ensure that you are familiar with POPI and PAIA and amendments made thereto or any other legislation that may be relevant and applicable to the processing of information or your appointment herein.

4. STAFF AWARENESS

4.1. All employees must attend a staff awareness session in respect of the POPIA and ensure that they understand:

4.1.1. What Personal Information is defined as;

4.1.2. The Life Cycle of Information that is processed;

4.1.3. The Processing Conditions as set forth by the Act;

4.1.4. The Penalties for Non-Compliance;

4.1.5. Direct Marketing under the Act;

4.1.6. General Understanding of the objectives envisaged by the Act.

4.2. Staff Awareness session will be compulsory for all to attend on an annual basis or as may be directed by the Information Officer from time to time.

5. COLLECTING OF INFORMATION OF CLIENTS

5.1. Personal Information may only be collected via the agency's systems; or

5.2. To which the staff member or agent is lawfully entitled to.

5.3. Information may only be collected in the following ways or as may be directed from time to time:

5.3.1. Directly from persons interested in using our services;

5.3.2. From third parties known to the person that have referred the client to us with the client's consent (in this case it must be made clear to the client on first contact who the third party is);

5.3.3. From a third party known to the person only where the third party has cleared consent to collect the information (or the agent's contact details can be given to the third party to be given to the client).

6. STORING INFORMATION

6.1. All personal information received and processed from a data subject must always be secured.

6.2. It remains the obligation of the agent or staff who is in possession of the personal information that it is correctly secured according to this internal policy.

6.3. **Hard copy** information, including mandates, offer to purchases, lease agreements or any other actual document with personal information of the data subject must always be:

6.3.1. Secured in a locked or secured in a folder or otherwise when not stored in the office.

6.3.2. Personal Information must be kept under lock in the office in the designated area or cabinet.

6.4. **Soft Copy** information must be stored electronically on a secured device. All devices must be secured as set out in this internal policy.

7. SHARING INFORMATION

7.1. Information may only be shared pursuant to the consent obtained by the client and includes sharing to:

7.1.1. The attorneys, conveyancers, advisers.

7.1.2. Mortgage originators, bond consultants

7.1.3. Agents or referral agents authorized thereto

7.1.4. Any other third party authorized thereto.

7.2. Information may not be shared with any other party not lawfully entitled to such information.

7.3. Information may only be shared for the purpose which it was consented to be shared for.

8. DELETING, ARCHIVING AND DESTROYING INFORMATION

8.1. Information requested by the client to be deleted or destroyed must be done as directed by the Information Officer.

8.2. All information to which the employee, staff or agent is not lawfully entitled to must be removed from the system with prior authorization from the Information Officer.

8.3. All hard copy documents that contain personal information in the office must be shredded or otherwise destroyed.

9. EMPLOYEE INFORMATION

9.1. All employees, staff and agent's information are confidential.

9.2. No information may be shared or otherwise processed unless lawfully entitled to do so and by the head or as otherwise directed.

9.3. Should any employee or staff member leave the employee of this agency, the agency will ensure that information is archived, destroyed or deleted as the case may be.

9.4. Sharing of employee information is strictly prohibited.

10. IT SECURITY

10.1. All employees, agents and staff must be familiar with the systems used by the agency.

10.2. Employees must ensure that their mobile devices and laptops are secured at all times.

10.3. Any theft or system breach of a mobile device must be reported immediately to the Information Officer.

10.4. The agency may request from time to time to inspect any and all mobile devices to ensure that the proper malware protection is installed on the devices, this may include malware protection, passwords and usernames.

10.5. Employees and staff are cautioned from using any "open" or "unsecured" Wi-Fi connections.