BUSINESS NAME: CAPE WATERFRONT ESTATES CLOSE CORPORATION
REGISTRATION NUMBER: CK 94/11478/23
OFFICE ADDRESS: 43 VICTORIA AVENUE, HOUT BAY, 7806
BUSINESS WEBSITE: www.capewaterfrontestates.co.za
PPRA NO: 2023115242

DATA PRIVACY TERMS AND CONDITIONS 2026

Document title:	DATA PRIVACY TERMS AND CONDITIONS – CAPE WATERFRONT ESTATES	Revision date:	4 SEPT 2026
Responsible Dept:	COMPLIANCE	Version No.:	5
Version compiled by:	MC COMPLIANCE CONSULTANTS	Version approval:	MARGIE ANN MACKENZIE & CLARE ELAINE PUTSMAN (effective on signature of the Implementation Resolution)
Applicable to:	MANAGEMENT, AGENTS AND DATA SUBJECTS (PUBLIC VERSION)	Pages:	47
Purpose:	To comply with the provisions of the Protection of Personal Information Act 4 of 2013, as amended, and its Regulations		
Last date audited:	AUGUST 2026	Document No.:	1
Last audited by:	MC COMPLIANCE CONSULTANTS	Level:	PUBLIC

1. PREAMBLE

1.1 Our agency has implemented a Data Privacy and Cyber Security Management framework in line with the South African Protection of Personal Information Act 4 of 2013 ("POPIA"), as amended by the Information Regulator's Amendment Regulations, 2025 (in effect from 17 April 2025).

1.2 Our agency's Data Privacy Terms and Conditions apply to all external and internal parties with whom we interact, including but not limited to clients, visitors to our offices, visitors to our website, visitors to external marketing portals to which we subscribe and where we list our client's properties, our own agents, employees and other users of our real estate services.

1.3 Who are our agency's data subjects and what type of information does the agency usually collect from these data subjects?

CATEGORY OF DATA SUBJECTS	PERSONAL INFORMATION WHICH IS COLLECTED AND PROCESSED
Prospective Clients	Names, identity numbers, email addresses, telephone numbers. IP addresses if enquiries are made via our agency's website or one of our chosen marketing portals
Clients	Names, addresses, registration numbers or identity numbers, employment status, marital status, telephone numbers, email addresses, nationality, citizenship, VAT numbers and bank details, tax numbers, source of income, source of funds, source of wealth, residency, citizenship, property ownership, mortgage bond particulars. IP addresses if enquiries are made via our agency's website or one of our chosen marketing portals
Service Providers	Names, registration numbers or identity numbers, VAT numbers, addresses, trade secrets and bank details. IP addresses if enquiries are made via our agency's website or one of our chosen marketing portals
Employees and potential employees	Names, surnames, identity numbers, addresses, qualifications, employment record, health records, criminal records, references, salary details, appointment letters, leave forms, disciplinary records, telephone numbers, marital status, spouse's telephone numbers, children's particulars, educational records, email addresses and records of employee life cycle, the Employment Equity plan, gender and race.
Debtors/ Creditors	Names, addresses, registration numbers or identity numbers, Statements, Invoices, bank details, telephone numbers, email addresses. IP addresses if enquiries are made via our agency's website or one of our chosen marketing portals

1.4 "Processing" of information encompasses a wide range of activities starting with the initial obtaining of personal information, proceeding to the use and retention of that information as well as access, disclosure of same and ending with its disposal.

1.5 As with most South African companies, our agency does communicate with data subjects cross-border and has considered the ISO27001 provisions, together with the requirements of the Cybercrimes Act 19 of 2020, in preparing our Data Privacy and Cyber Security Management framework.

1.6 We process personal information only where we have a lawful basis to do so under Section 11 of POPIA. Depending on the circumstances, this may include your Consent, the performance of a contract to which you are party, compliance with a legal obligation (such as our duties under FICA, the Property Practitioners Act or tax legislation), or the legitimate interests of our agency or a third party, provided your interests, rights and freedoms are not thereby overridden. Where our processing relies on your Consent, you have the right to withdraw that Consent at any time as set out in clause 10 below.

1.7 In delivering our real estate services, our agency respects the privacy of your personal information, and we have implemented reasonable measures to ensure that processing of your personal information is aligned to the requirements of POPIA.

1.8 In this document we explain how and when we process personal information.

1.9 If you have questions arising from the processing of information that are not specifically listed herein, you may contact our agency's Information Officer, margie@capewaterfrontestates.co.za for assistance, or lodge a request via our agency's data subject request channels described in clause 10 below.

1.10 The agency's data security mitigation measures are governed by the following internal and external policies. Only documents expressly identified as external are made available publicly. Internal policies, schedules and plans, including Annexure A (Cyber Security Measures) and the Disaster Recovery Rules, are maintained separately for authorised internal use and are not published:

Data Privacy Terms and Conditions	External Policy made available to our agency's data subjects via our agency's website and available from the Information Officer: margie@capewaterfrontestates.co.za
Data Classification Policy	Internal Policy
Internal IT and Email Usage Policy	Internal Policy
Data Incident Reporting Policy	Internal Policy
Payments Policy	Internal Policy
Employee Data Consent and Accountability Declaration	Internal declaration
Conflict of Interest Policy	Internal Policy
Data Archiving and Record Keeping Policy	Internal Policy
Client Consent (Once off engagement / Ongoing engagement)	External Consent to be signed by every one of the agency's clients at onboarding
Supplier Consent (Once off engagement / Ongoing engagement)	External Consent to be signed by every one of the agency's suppliers, irrespective of the supply
Professional Associates' Declaration (ongoing association)	External declaration to be signed by professional associates who engage with the agency on an ongoing basis
Professional Associates' Declaration (once off association)	External declaration to be signed by professional associates who engage with the agency on a once off basis
Third Party Operator's Agreement and Non-Disclosure	External agreement to be signed by suppliers who process data on behalf of the agency

The agency's Business Continuity Plan	Internal plan
PAIA Manual	External manual made available to our agency's data subjects via the agency's website and available from the Information Officer – margie@capewaterfrontestates.co.za
Our agency's Website Usage Policy	External Policy published on our agency's website
Updated email disclaimers	Embedded on emails sent from the agency

1.11 Our agency may review and update our Data Privacy Terms and Conditions, and other Policies associated thereto, from time to time to ensure ongoing compliance with POPIA, its Regulations, and guidance issued by the Information Regulator.

1.12 Where the provision of your personal information to our agency is mandatory (for example, because it is required by FICA, the Property Practitioners Act or other legislation, or is necessary to conclude or perform a contract with you), we will make this clear at the time of collection, together with the possible consequences of not providing that information, which may include our being unable to proceed with your instruction, application or transaction. Where provision of information is voluntary (for example, for newsletters or optional marketing), this will also be made clear.

1.13 Where our agency intends to transfer your personal information to a recipient outside of South Africa, we will only do so in accordance with Section 72 of POPIA, and, where applicable, we will inform you of the transfer and of the safeguards or basis relied upon.

1.14 Effective 6 March 2026, the Information Regulator's Regulations on the Processing of Data Subjects' Health Information by Certain Responsible Parties, 2026 (published in Government Gazette No. 54268) apply to employers, including our agency, that process employees' health information. Where our agency processes an employee's or job applicant's health information (as reflected in clause 1.3 above), we do so subject to an obligation of confidentiality, we maintain appropriate technical and organisational safeguards to protect its confidentiality, integrity and availability, we dispose of such records securely in accordance with clause 9 below, and we do not transfer such information across South Africa's borders other than in accordance with Section 72 of POPIA and these Regulations.

1.15 If you believe that our agency has processed your personal information unlawfully, you have the right to lodge a complaint with our Information Officer in the first instance, and thereafter with the Information Regulator. Full details of this right, and how to exercise it, are set out in clause 10 below.

2. INTRODUCTION

2.1 Our agency specialises in property sales and rentals involving properties mostly, but not exclusively, situated in the Cape Town Atlantic Seaboard, Hout Bay, Llandudno and Constantia.

2.2 Our agency operates from one branch which is situated in the Hout Bay area.

2.3 In delivering our real estate services, our agency has to collect and process personal information as and when required, including but not limited to:

2.3.1 Our agency complying with Regulatory requirements, in terms of the Property Practitioners Act 22 of 2019 and the Property Practitioners Regulatory Authority ("PPRA"), the Consumer Protection Act and the Financial Intelligence Centre Act – amongst others;

2.3.2 The management of client enquiries, instructions or transactions in which we act or have received instruction or are involved with in any way on a professional basis;

2.3.3 When you browse our website or any of our listings on our agency's chosen marketing platforms, but we will not record any of your personal details from the website or from these marketing platforms unless you specifically subscribe or engage with us directly from the website or marketing platforms. These details are recorded in our website terms and conditions.

2.4 We may collect or obtain your personal information:

2.4.1 Directly from you;

2.4.2 In the course of our business relationship with you;

2.4.3 In the course of providing our services to you;

2.4.4 When you make your personal information public;

2.4.5 When you visit and/or interact with our website or our social media platforms;

2.4.6 When you register to access our services including but not limited to newsletters, information updates and similar services and products that we offer;

2.4.7 When you visit our offices; and

2.4.8 From third parties involved in your transaction.

2.5 We may record personal information about you such as records of your communications and interactions with us, including, but not limited to, your email and other communications with us, your details supplied for delivery of our services or goods (such as invoicing and other such information) or at interviews in the course of applying for a job with us, subscription to our newsletters and other mailings and interactions with you during the course of digital or 'in person' marketing campaigns.

2.6 We treat your personal information confidentially where required and only use, share, record or delete it as is required by law, as part of our service delivery to you and/or as lawfully instructed by you.

2.7 We primarily use your personal information only for the purpose for which it was originally or primarily collected.

2.8 In line with Section 15 of POPIA, we will only use your personal information for a further (secondary) purpose where that further processing is compatible with the purpose for which it was collected, having regard to factors such as the relationship between the purposes, the nature of the information concerned, how the information was obtained, the consequences of the intended further processing for you, and the extent to which we have contractually agreed to further conditions of processing. Where further processing would not be compatible with the original purpose, we will only proceed with your Consent or where another basis under POPIA applies.

3. OBJECTIVE OF THESE TERMS AND CONDITIONS

3.1 Although it is not possible to ensure 100% mitigation against data breaches, the objective of our agency's Data Privacy Terms and Conditions is to ensure adherence by our agency and all agents and employees associated with our agency, to the provisions within POPIA together with its Regulations, as amended.

3.2 It is a priority for our agency to continue to create Management direction and high-level objectives for regulating the manner in which personal information is processed and to provide for remedies in cases where personal information is not handled accordingly.

3.3 Further purposes of this Policy include:

3.3.1 The supplementation of all our agency's Policies and procedures related to the handling of data subjects' information and to align it with South African laws;

3.3.2 General compliance with the requirements of POPIA;

3.3.3 The identification and codification of documents and ensuring adequate protection and maintenance of accuracy of documents where required;

3.3.4 Providing a set framework and unified Policy regarding the methods and procedures for the retention and destruction of documents;

3.3.5 Ensuring that data subjects' Consent is obtained as provided for in POPIA;

3.3.6 Ensuring that our agency's data subjects' information is not unlawfully shared with third parties unless Consent for such sharing is obtained or that the sharing is lawful;

3.3.7 Protecting all of our agency's data subjects from harm;

3.3.8 To stop identity fraud;

3.3.9 Ensuring records that are no longer required or documents that are of no value are destroyed properly and in accordance with the data retention schedule; and

3.3.10 Aiding agents and employees in understanding the requirements relating to the protection of personal information and the retention and destruction of documents.

Our aim is to add as many data risk mitigation measures as possible to our data protection arsenal

4. THE VALUE OF INFORMATION TO OUR AGENCY

4.1 One of the fundamental principles of information security is “need to know”. This applies to both the agency's handling of information and how the information is processed.

4.2 This “need to know” principle means that information collected and processed by the agency shall be disclosed only to those people who have a legitimate and approved business need for the information.

4.3 Inappropriate handling of information could expose the agency to the following risks:

4.3.1 **Financial Exposure:** Disclosure could cause varying scale of financial loss depending on how the asset loss impacts business;

4.3.2 **Legal/Contractual/ Regulatory Compliance Liability:** Certain kinds of non-compliance may lead to a legal or Regulatory exposure. Its severity could place senior Management in direct line of liability;

4.3.3 **Reputation:** Certain information assets could be put to malicious use by journalists, activists, alienated clients, alienated agents or employees. The intent in such cases could be to hurt the confidentiality integrity and availability of assets that build brand value;

4.3.4 **Value to the Competition:** Loss of certain assets to a competitor could put the agency to a competitive disadvantage over a period of time. This loss could undermine the agency's market position and share; and

4.3.5 **Personnel Motivational Impact:** Information such as compensation packages, performance appraisals or complaints and grievances, could adversely impact agent and employee relations.

4.4 The agency will draw a comprehensive list of information assets on which information is processed, used and stored including but not limited to: (soft & hard) hardware, software, people and outsourced services shall also be done by the agency on an annual basis.

4.5 Our agency's data is categorised into the following different classifications presented in order of increasing sensitivity:

INFORMATION DESCRIPTION	EXAMPLES	CATEGORY
UNCLASSIFIED PUBLIC	Public data refers to information that is meant for public consumption and does not pose any risk or harm if disclosed. Public data is considered non-sensitive and can be freely shared without significant concern for confidentiality. This category includes information that is intentionally made available to the general public, such as press releases, marketing materials, and publicly accessible information or documents.	Product brochures widely distributed. Information widely available in the public domain, including publicly available website areas. Newsletters for external transmission
PROPRIETARY	Internal data encompasses information that is essential for the functioning of the agency but may not be as sensitive as confidential data. It is intended for use	Passwords and information on corporate security procedures. Know-how used to process client information. Standard Operating

	within the agency and is not meant for public disclosure. Internal data may include project plans, internal communications, and certain operational details. Information restricted to Management, approved internal access and protected from external access. Unauthorized access could influence operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in client confidence. Information integrity is vital.	Procedures used in all parts of our agency's activities. All software codes developed by our agency whether used internally or sold to clients.
CONFIDENTIAL	Confidential data refers to information that is highly sensitive and should be handled with the utmost care. Unauthorized access, disclosure, or modification of confidential data can have severe consequences. This category often includes personal identification information, financial data, trade secrets, and other critical proprietary information. Information collected and used by the agency in the conduct of its business to employ people, to log and fulfil client mandates, and to manage all aspects of corporate finance. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	Salaries and other personnel data. Accounting data and internal financial reports. Confidential client business data and confidential contracts. Non-disclosure agreements with clients/ vendors. Company business plans. Emails with clients and suppliers. Personal and special personal information and copies of documents supplied to the agency by clients. Banking details

4.6 Our agency's information list hereunder contains a summary of the majority of data which is collected, processed, used and stored during the course of our operations and this list has been categorised, for ease of reference according to the value of such data and information:

TYPE OF RECORDS	DETAILED EXAMPLES	CLASSIFICATION
BUSINESS ACCOUNTING RECORDS	◦ Annual financial statements and working papers ◦ General ledger ◦ Bank statements, cheque books, cheques ◦ Client and supplier statements and invoices ◦ Deposit slips ◦ Cash books and petty cash books ◦ Fixed asset register ◦ Tax returns and assessments ◦ VAT returns ◦ Lease or instalment sale agreements ◦ Budgets and business plans ◦ Insurance records ◦ Auditor's reports (internal, compiler's, accounting officer's, reviewer's) ◦ Inventory records (including stock take)	PROPRIETARY

	◦ Systems documentation ◦ Management reviews ◦ Capital expenditure ◦ Record of assets, liabilities, loans to related parties, obligations, property held, revenue and expenses	
CREDIT AGREEMENTS	◦ Credit Provider's documents	PROPRIETARY
FIXED PROPERTY	◦ Leases ◦ Mortgage bonds or other encumbrances ◦ Title deeds	PROPRIETARY
HEALTH AND SAFETY	◦ Evacuation Report ◦ Minutes of safety committee meetings (if any)	CONFIDENTIAL
INFORMATION TECHNOLOGY AND SYSTEMS	◦ Hardware ◦ Internet ◦ Software packages ◦ Telephone exchange equipment ◦ Telephone lines, leased lines and data lines	PROPRIETARY
PROFESSIONAL AND OTHER INSURANCE	◦ Claim records ◦ Details of coverage, limits and insurers ◦ Insurance policies	PROPRIETARY
LEGAL AGREEMENTS	◦ Contracts with Clients ◦ Contracts with Employees ◦ Contracts with External Service Providers ◦ Contracts with Suppliers with shareholders, officers or members	CONFIDENTIAL
PERSONNEL RECORDS (HUMAN RESOURCES)	◦ Disciplinary records ◦ Employee information records ◦ Employee loans ◦ Employee remuneration ◦ Employment applications ◦ Employee date of birth ◦ Employment contracts ◦ Group personal accident ◦ IRP 5 and IT 3 certificates ◦ Letters of appointment ◦ Leave applications ◦ Maternity leave Policy ◦ Payroll ◦ Particulars of each employee and agent ◦ Personnel file ◦ Recruitment and appointments ◦ Salary and wage registers ◦ Salary slips and wage records ◦ Tax returns of employees and agents ◦ Training and development ◦ UIF, PAYE and SDL returns ◦ Workmen's Compensation documents	CONFIDENTIAL
MARKETING	◦ Newsletters	PROPRIETARY

	◦ Service and product information ◦ Client onboarding details ◦ Marketing agreements ◦ Debt Acknowledgement ◦ Invoices, Credit notes	
INTELLECTUAL PROPERTY	◦ Templates ◦ Digital and physical publications ◦ Internal and External Compliance Policies	CONFIDENTIAL
STATUTORY COMPANY RECORDS	◦ Annual Statutory Returns ◦ Certificate of Change of Name ◦ Certificate of Incorporation ◦ Certificate to Commence Business ◦ Dividend register ◦ Members' attendance register ◦ Founding Statement and Association Agreement ◦ Notice and minutes of members' meetings ◦ Proxy documents ◦ Resolutions ◦ Members' agreements ◦ Members' register	PROPRIETARY
TAX	◦ Income tax returns ◦ Provisional tax returns ◦ Tax assessments ◦ VAT documents	PROPRIETARY
THIRD PARTIES	◦ Section 71 of PAIA makes provision for a request for information or records about a third party. ◦ In considering such a request, the agency will adhere to the provisions of Sections 71 to 74 of PAIA. ◦ In certain circumstances, the agency will be obliged to advise third parties of requests lodged in respect of information applicable to or concerning such third parties. ◦ In addition, the provisions of Chapter 2 of Part 4 of PAIA entitle third parties to dispute the decisions of the head of the agency or the request liaison officer by referring the matter to the High Court.	CONFIDENTIAL

5. POPIA CORE PRINCIPLES

In our quest to ensure that we protect, as far as we are able to do so, our data subjects' data privacy, our agency fully commits as follows:

5.1 To continue developing and maintaining reasonable protective measures against the possibility of risks such as loss, unauthorised access, destruction, use, alteration or revelation of personal information.

5.2 To regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information.

5.3 To ensure that the requirements of the POPIA legislation are upheld within our agency. In terms of Sections 8, 17 and 18 of POPIA, our agency adheres to an approach of transparency of operational procedures that controls collection and processing of personal information and subscribes to a process of accountability and openness throughout its operations.

5.4 In terms of the requirements set out within Sections 9, 10, 11, 12, 13, 14 and 15 of POPIA, to only collect personal information in a legal and reasonable way, for a specific reason and only if it is necessary for our operations and to process the personal information obtained from clients, agents, employees, visitors and service suppliers only for the purpose for which it was obtained in the first place.

5.5 Not to process personal information obtained from clients, our agents, our employees, visitors and service providers in an insensitive, derogative, discriminatory or wrongful way that can intrude on the privacy of the particular data subject.

5.6 In terms of the provisions contained within Sections 23 to 25 of POPIA, and the Information Regulator's Amendment Regulations, 2025, to allow all data subjects of our agency the right to request access to certain personal information and correction or deletion of personal information within the specifications of the POPIA. Requests for objection, correction or deletion are dealt with free of charge and may be submitted through any reasonably accessible channel, including email, post, fax, hand-delivery, SMS or WhatsApp. Data subjects should refer to ANNEXED FORMS 1 & 2 attached hereto for these purposes.

5.7 Not to request, or process, special personal information (such as information related to race, religion, medical situation, political preference, trade union membership or sexual orientation) or information concerning criminal behaviour, except where permitted under Sections 26 to 33 of POPIA – for example, with the data subject's express Consent, where necessary to establish, exercise or defend a right or obligation in law, where the information has deliberately been made public by the data subject, or where another exception recognised by POPIA applies. Our agency will also not process the personal information of a child unless one of the grounds set out in Section 35 of POPIA, including the specific Consent of a competent person, applies.

5.8 In terms of the provisions contained within Section 16 of POPIA, to continue to be committed to ensuring that data subjects' information is recorded and retained accurately.

5.9 Not to provide any documentation to a third party or service provider without the express Consent of the data subject, except where the disclosure is necessary for the proper execution of the service as expected by the data subject, or is otherwise required or permitted by law (for example, our statutory duties under FICA or the Property Practitioners Act).

5.10 To keep effective record of personal information and, in accordance with POPIA's retention limitation condition, to retain information for no longer than is necessary to achieve the purpose for which it was collected or processed, unless a longer period is required or permitted by law.

5.11 In terms of Sections 19 to 22 of POPIA, and the Cybercrimes Act 19 of 2020, to ensure the integrity and confidentiality of personal information in our possession and to provide the necessary security of data and keep it in accordance with prescribed legislation.

5.12 To comply with the Information Regulator's Amendment Regulations, 2025, including: processing objection, correction and deletion requests free of charge and through accessible channels; responding to such requests in writing within 30 days; and only relying on Consent for direct marketing where that Consent is an unambiguous opt-in action – pre-ticked boxes, silence or inaction do not constitute valid Consent, and telephonic Consent must be recorded and made available to the data subject on request.

6. COLLECTION AND PROCESSING OF PERSONAL INFORMATION

As referenced in clauses 2.3 and 2.4 above, our agency may subject your personal information to processing during the course of various activities, including:

6.1 The general operation of our agency in facilitating property enquiries and enabling property transactions;

6.2 Analysis, evaluation, review and collation of information in order to determine potential disputes, provide project advice and preparing or commenting on opinions, project projections, responding to correspondence, reports, publications, documents relating to our projects and any other documents and records;

6.3 Compliance with the law and specifically fraud prevention and the combatting of money laundering;

6.4 Transfer of information to our service providers and operators;

6.5 For recruitment purposes;

6.6 For relationship management and marketing purposes in relation to our services (including, but not limited to, processing that is necessary for the development and improvement of our services), for accounts management, and for marketing activities in order to establish, maintain and/or improve our relationship with you;

6.7 In addition, we may process your personal information for statistical purposes and for internal management and Management reporting purposes, including but not limited to: conducting internal audits, conducting internal investigations, implementing internal business controls, providing central processing facilities, for insurance purposes and for Management reporting analysis;

6.8 We may process your personal information for safety and security purposes;

6.9 We may share certain personal information with other institutions as part of our service rendering or as legally required, such as sharing information with the Receiver of Revenue, local authorities, the courts, sheriffs and the like. We only share such personal information as are required for fulfilling our service mandate or as prescribed by law.

6.10 Collection of personal information from another source may be necessary –

6.10.1 To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

6.10.2 To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue;

6.10.3 For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;

6.10.4 In the interest of national security;

6.10.5 To maintain the legitimate interests of our agency or of a third party to whom the information is supplied;

6.10.6 Where compliance would prejudice a lawful purpose of the collection;

6.10.7 Where compliance is not reasonably practicable in the circumstances of a particular contract.

6.11 Our agency often collects personal information from other parties involved in our transactions as various role players often share clients in a single transaction.

6.12 Most of our communications are done electronically via the internet, per email and other electronic methods and we recognise the international risk of data and email breaches.

6.13 To ensure that lawful conditions exist surrounding our data subject's information, we accept that all its South African based data subjects' Constitutional Right to Privacy is of utmost importance and that our data subjects based in other parts of the world are equally entitled to rights to privacy in terms of Regulations applicable to such data subjects in the countries in which they are based.

6.14 As such, we are committed to comply with South Africa's POPIA provisions, as amended, and to the education of our data subjects in respect of your rights to privacy and to make all operational amendments necessary.

7. CONSENT

7.1 When our data subjects' information is collected, processed or shared by our agency, it will be on one or more of the lawful grounds recognised by Section 11 of POPIA: your Consent, the performance of a contract with you, compliance with a legal obligation such as FICA, the Property Practitioners Act or tax legislation, or the legitimate interests of our agency or a third party. This clause 7 deals in particular with the instances where we rely on your Consent.

7.2 Where our processing of a particular category of information relies on Consent rather than another lawful ground, we explain the reasons for the collection of information from the particular data subject/s and obtain the required Consents to process, and where required, for the sharing of information pursuant to such explanation.

7.3 We may process the following categories of Personal Information about you:

7.3.1 Personal details: name, identity number / passport number and photograph;

7.3.2 Demographic information: gender; date of birth / age; nationality; salutation; title; language preferences;

7.3.3 Contact details: correspondence address; telephone number; email address; details of your public social media profile(s); utility provider details;

7.3.4 Transactional details: details of individuals transacting with us;

7.3.5 Personal Information included in correspondence, documents, evidence or other materials that we process while providing our services and/or acquiring or selling property;

7.3.6 Attendance records: details of meetings and other events organised by us that you have attended;

7.3.7 Consent records: records of any Consents you may have given, together with the date and time, the means of Consent and any related information;

7.3.8 Payment details: billing address; payment method; bank account number or credit card number; invoice records; payment records; SWIFT details; payment amount; payment date; bank statements;

7.3.9 Data relating to your visits to our website: your device type; operating system; browser type; browser settings; IP address; language settings; dates and times of connecting to a website; and other technical communications information;

7.3.10 Your employer details: where you interact with us in your capacity as an agent or employee, the name, address, telephone number and email address of your employer, to the extent relevant.

7.4 Our agency understands the importance of obtaining our data subjects' Consent where necessary to share their information and possibly using the information for limited marketing purposes.

7.5 If personal information is used for any other reason than the original reason of it being collected, the specific Consent for such purpose will be obtained from the data subject.

7.6 Further processing of personal information must be compatible with the purpose of collection, unless the data subject has Consented to such further processing.

7.7 Where personal information is transferred to a third party for further processing, the further processing must be compatible with the purpose for which it was initially collected, unless the data subject has Consented to such further processing or it is permitted in terms of POPIA.

7.8 If personal information is to be used for any other purpose the further Consent of the data subject must be obtained. Where this is not possible, the Information Officer should be consulted.

7.9 Our agency does not use information for other purposes other than what it was collected for.

7.10 If special personal information is collected, processed and stored for any reason from any of our agency's data subjects, a specific Consent for such collection will first be obtained.

7.11 There are instances in which this specific Consent will not be required:

7.11.1 If collection and processing are carried out with a prior Consent of the data subject;

7.11.2 If collection and processing are necessary for the establishment, exercise or defence of a right or obligation in law;

7.11.3 If collection and processing are for historical, statistical or research purposes;

7.11.4 If we are obliged to collect and process your information in terms of regulation.

7.12 Our agency's standard documentation reflects the Consent mechanisms required by POPIA, as amended by the POPIA Amendment Regulations, 2025 – namely that Consent must be given through a clear, affirmative, opt-in action, that pre-ticked boxes and silence do not constitute valid Consent, and that Consent obtained telephonically is recorded and retained.

7.13 In as far as the conflict which often arises when the agency performs its FICA (Financial Intelligence Centre Act 2001 (“FICA”) as amended) duties and clients' expectations of their information being kept secret by the agency, it is acceptable that the agency collects, processes, stores and shares a lot of personal and special personal information from clients, in particular financial information, in order to fulfil its statutory FICA duties, including client due diligence, beneficial ownership verification and screening against targeted financial sanctions lists.

7.14 The question is always: was the collection, processing and storage of information lawful and necessary to address the possible money-laundering and terrorist-financing risks in the agency's transactions?

7.15 As long as the agency does not overstep the lawful line allowed by FICA for collection and assessment of client information without their specific Consent, the agency will enjoy the Financial Intelligence Centre's protection.

7.16 FICA clarifies the issue of data privacy of clients for the agency, who will often be collecting, verifying and screening client information from third party sources without a specific Consent form such client.

7.17 While the processing and further processing of personal information of a client for purposes of FICA requirements is allowed in terms of POPIA, the agency should be cautious of verifying clients' juristic clients using third party data sources which may have obtained personal information about a client without the client's Consent or knowledge.

7.18 In this regard, CLEAR NOTICE must be supplied in the agency's FICA questionnaires in respect of the agency's lawful FICA duties and that information collected for fulfilment of duties set out in the FICA will

be dealt with confidentially within the confines of the responsibility to report such information to the FIC where necessary.

7.19 The Information Officer for the agency will ensure at all times that the processes are followed as set out in the agency's FICA Policy and that she will control the processes and ensure compliance with the need to keep information confidential.

7.20 The agency acknowledges SECTION 37(1) of the FIC Act, which states that no duty of secrecy or confidentiality or any other restriction on the disclosure of information, whether imposed by legislation or arising from the common law or agreement, affects compliance by the agency to report to the FIC.

7.21 In terms of SECTION 41A of the FIC Act, the FIC will ensure that it has appropriate measures in place to protect the confidentiality of personal information received by establishing and maintaining appropriate safeguards against the foreseeable internal and external risks identified.

7.22 In line with the Information Regulator's Guidance Note on Direct Marketing (December 2024), where the agency approaches a data subject who is not an existing client to obtain Consent for direct electronic marketing (including telephone calls, which the Regulator treats as electronic communications), the agency will only approach that data subject once, will not do so if Consent has previously been refused, and every direct marketing communication will identify the sender and provide the data subject with a means to opt out free of charge.

8. STORAGE OF INFORMATION

8.1 Management of our agency and all agents and employees of our agency remain aware of the risks facing data subjects with the storage of personal and special personal information on our agency's software systems as well as filing copies of the physical information sheets containing personal information physically in our office.

8.2 Our agency stores personal information in its possession:

8.2.1 At our business premises, in the form of hard copies where necessary;

8.2.2 On our agency's physical and cloud-based servers; or

8.2.3 On the servers of third-party service providers, such as IT systems or hosting service providers.

8.3 Our agency will continuously take reasonable technical and organisational measures to secure the integrity of data in our possession. This includes adopting technological standards to prevent unauthorised access to or disclosure of data, guarding against the offences created under the Cybercrimes Act 19 of 2020, and protecting information of data subjects from misuse, loss, alteration and destruction.

8.4 Periodical reviews of our agency's personal information practices and processes regarding collection, storage and technical security measures will be conducted.

8.5 Our agency will ensure that the contracts between itself and third-party service providers and/or contractors and sub-contractors are updated regularly to secure the integrity and confidentiality of personal information in our possession.

8.6 In accordance with Section 14 of POPIA, our agency will not keep records of personal information for longer than is necessary to achieve the purpose for which the information was collected or subsequently processed. Retention periods are principally determined by applicable legislation, including FICA, the Property Practitioners Act, tax and employment legislation, and our internal Record Keeping and Archiving Policy; a longer retention period may also apply where the data subject has specifically consented or instructed our agency to retain particular records for longer, or where retention is otherwise necessary for a legitimate business or legal purpose such as pending or reasonably foreseeable litigation.

8.7 To ensure that our best attempts are made to minimize data subjects from suffering loss of personal information, misuse or unauthorised alteration of information, unauthorized access or disclosure of personal information generally, we will:

8.7.1 Store personal information in databases that have built-in safeguards and firewalls to ensure the privacy and confidentiality of your information.

8.7.2 Constantly monitor the latest internet developments to ensure that the systems evolve as required. Our agency tests our systems regularly to ensure that our security mechanisms are up to date.

8.7.3 Continue to review our internal policies and third-party agreements where necessary to ensure that these are also complying with the POPIA and Regulations in line with our agency's general Data Privacy Terms.

8.8 Our agency is subject to the record keeping requirements provided in many South African laws, including but not limited to: the Property Practitioners Act, the Financial Intelligence Centre Act, the Income Tax Act and The Companies Act of South Africa.

To this end and to be sure that we comply with regulatory record keeping duties, our agency has developed and implemented our Record Keeping And Archiving Policy which is reviewed regularly.

9. DISPOSAL OF DATA SUBJECTS' INFORMATION

9.1 As provided for in our agency's Record Keeping And Archiving Policy, our agency commits to its responsibility to ensure that records that are no longer needed or are of no value are disposed of at the proper time.

9.2 These rules apply to all documents and information which are collected, processed or stored by our agency and include but are not limited to documents in paper and electronic format, for example, e-mail, web and text files and PDF documents etc.

9.3 Our agency's Record Keeping And Archiving Policy determines when and how information and communications with and to our clients are kept and stored and when information would be destroyed including but not exclusively limited to:

9.3.1 How emails are stored and when emails are deleted destroyed;

9.3.2 How client data is stored, on which software systems and when these are destroyed;

9.3.3 How physical copies of information and communications are stored and when these are destroyed;

9.3.4 How our software and hardware products are monitored and appropriate rules implemented with regards to storage of data subjects' information hereon.

9.4 As a matter of course, we do not discard or dispose of the telephone numbers, email addresses and electronic communications with data subjects with whom we have previously dealt but will do so on request by the data subject.

9.5 However, since our agency recognizes that most of the information which it collects, processes and shares with other role players in transactions is personal of nature, we do not let information lie around and keep strict controls in respect of access to our software systems.

9.6 For this reason, we will dispose of information securely when no longer required or when being requested by the data subject.

9.7 Our agency acknowledges that electronic devices and media hold vast amounts of information, some of which can linger indefinitely, and we follow the following rules strictly:

9.7.1 Under no circumstances will paper documents or removable media (CD's, DVD's, discs, etc.) containing personal or confidential information be simply binned or deposited in refuse tips.

9.7.2 Our agency will ensure that all electrical waste, electronic equipment and data on disk drives are physically removed and destroyed in such a way that the data will by no means be able to be virtually retrieved.

9.7.3 Our agency will also ensure that all paper documents that should be disposed of, be shredded locally and then be recycled.

9.7.4 In the event that a third party is used for data destruction purposes, our agency's Information Officer will ensure that such third party also complies with our rules and any other applicable legislation.

9.8 Our agency may suspend the destruction of any record or document due to pending or reasonably foreseeable litigation, audits, government investigations or similar proceedings and we undertake to notify all agents and employees of applicable documents where the destruction has been suspended to which they have access.

9.9 In the event that a document and/or information is no longer required to be stored in accordance with either legislation or in line with our own rules, it should be deleted and destroyed.

9.10 Our agency's Information Officer will give direction where there is uncertainty regarding the retention and destruction of a document and/or information.

10. OUR AGENCY'S DATA SUBJECTS' RIGHTS

10.1 Our agency recognises that our data subjects have the right to request that our agency confirms, free of charge, whether or not it holds personal information about the data subject and request the agency to provide a record, or a description of the personal information held, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information.

10.2 All of our agency's data subjects, or a competent person where the data subject is a child, may withdraw his, her or its Consent to procure and process his, her or its personal information, at any time, providing that the lawfulness of the processing of the personal information before such withdrawal or the processing of personal information not affected.

10.3 Any of our data subjects may object, at any time, to the processing of personal information –

10.3.1 In writing, on reasonable grounds relating to his, her or its particular situation, unless legislation provides for such processing; or

10.3.2 For purposes of direct marketing other than direct marketing by means of unsolicited electronic communications.

10.4 All of our data subjects, having provided adequate proof of identity, have the right to –

10.4.1 Request from us to confirm, free of charge, whether we hold personal information about the data subject; and

10.4.2 Request from our agency a record or a description of the personal information about the data subject held by us including information about the identity of all third-parties, or categories of third-parties, who have, or have had, access to the information – within a reasonable time; at a fee that may be prescribed under PAIA for reproduction only, and never for the request itself; in a reasonable manner and format; and in a form that is generally understandable.

10.5 Our data subjects may, in the prescribed manner and free of charge, request our agency to –

10.5.1 Correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or

10.5.2 Destroy or delete a record of personal information about the data subject that our agency is no longer authorised to retain.

10.6 Upon receipt of a request referred to in clause 10.5, our agency will, within 30 days of receipt of the request –

10.6.1 Correct the information;

10.6.2 Destroy or delete the information;

10.6.3 Provide the data subject, to his, her or its satisfaction, with credible evidence in support of the information; or

10.6.4 Where an agreement cannot be reached between our agency and the data subject, and, if the data subject so requests, take such steps as are reasonable in the circumstances, to attach to the information, in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made.

10.7 Our agency will inform the data subject, who made a request as set out in clause 10.5, in writing, of the action taken as a result of the request, within 30 days as required by the Information Regulator's Amendment Regulations, 2025.

10.8 All users will comply with our agency's data subject access request Policy and PAIA manual in respect of any access to personal information requests by data subjects.

10.9 Our agency will provide credible proof to the individual of the action that has been taken in response to the request. If any changes to the personal information will have an impact on any decisions to be made about the individual, the agency will inform all third parties to whom the information has been disclosed, including any credit bureaus, of such changes.

10.10 A request under this clause may be submitted through any reasonably accessible channel, including email, post, fax, hand-delivery, SMS or WhatsApp, addressed to the Information Officer.

10.11 Please refer to ANNEXED FORM 1 of the POPIA Regulations attached hereto should you wish to object to the processing of your Personal Information.

10.12 Please refer to ANNEXED FORM 2 of the POPIA Regulations attached hereto should you wish to request the correction or deletion of your Personal Information.

10.13 Right to complain to the Information Regulator: if you are unhappy with how our agency has processed your personal information, we encourage you to raise the matter with our Information Officer first, using the contact details in clause 15 below, so that we have the opportunity to resolve it. You also have the right, in terms of Section 5(h) and Section 74 of POPIA, to lodge a complaint directly with the Information Regulator at any time. Complaints are lodged via the Information Regulator's eServices Portal (https://eservices.inforegulator.org.za), using Form 5 of the Regulations, or by contacting the Information Regulator directly:

Physical address:	Woodmead North Office Park, 54 Maxwell Drive, Woodmead, Johannesburg, 2191

Email:	enquiries@inforegulator.org.za / complaints.IR@justice.gov.za
Telephone:	010 023 5200 / Toll-free: 0800 017 160
Website:	www.inforegulator.org.za

As these details may change from time to time, data subjects should confirm current contact details on the Information Regulator's website before submitting a complaint.

11. CYBER TECHNOLOGY

11.1 Standard Anti-Virus rules

11.1.1 In order to ensure that our agency's IT systems are not misused and in accordance with our agency's Internal Devices, Email And Internet Usage Policy as well as our agency's Business Continuity And Disaster Recovery Plan, everyone who uses or has access to our systems have received training and internal guidelines in order to meet the following five high-level IT Security requirements:

11.1.1.1 Information will be protected against any unauthorized access as far as possible;

11.1.1.2 Confidentiality of information will be assured as far as possible;

11.1.1.3 Integrity of information will be preserved as far as possible;

11.1.1.4 Availability of information for business processes will be maintained;

11.1.1.5 Compliance with applicable laws and regulations to which our agency is subject will be ensured by our Information Officer as far as possible.

11.1.2 Every user of our IT systems takes responsibility for exercising good judgment regarding reasonable personal use.

11.1.3 Management of our agency is responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into our agency's programs (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited.

11.1.4 Our agency's agents and employees are discouraged from attempting to remove viruses themselves. If a virus infection is detected, users are expected to disconnect from our agency's networks, stop using the infected computer immediately and notify the IT support.

11.1.5 It is further worth noting that our agency's users are encouraged to be cautious of e-mail attachments from an unknown source as viruses are often hidden in attachments.

11.1.6 Our agency has entered into confidentiality agreements with every staff member to ensure full confidentiality in respect of all of our clients' affairs, including our clients' Personal Information.

11.1.7 Employees are trained to notify their manager/supervisor immediately if there are reasonable grounds to believe that the personal information of a client has been accessed or acquired by any unauthorised person.

11.1.8 The digital work profiles and privileges of staff who have left our employ are being properly terminated.

11.1.9 All agents and employees have received and will continue to receive internal training in respect of such viruses and how to identify them and what to do if a virus is suspected.

11.2 IT Access Control

11.2.1 Only authorized agents and employees may log into our agency's IT system and software packages, and these are password controlled.

11.2.2 All agents and employees of our agency exercise caution in allowing unauthorized access to a password and our agency's IT department ensure that the passwords are reviewed and renewed from time to time - in particular where GOOGLE based products are used and linked (such as Facebook, WhatsApp and GMAIL based domains).

11.3 Email Rules

11.3.1 Most of our agency's digital communications are conducted via email and instant messaging (IM).

11.3.2 Given that email and IM may contain extremely sensitive and confidential information, the information involved must be appropriately protected. In addition, email and IM are potentially sources of spam, social engineering attacks and malware.

11.3.3 The misuse of email and IM can pose many legal, privacy and security risks, so it is important for users of our agency's services to be aware of the appropriate use of electronic communications.

11.3.4 It is of use to note that all users of our agency's agents and employees are prohibited from using email to:

11.3.4.1 Send, receive, solicit, print, copy, or reply to text, images, or jokes that disparage others based on their race, religion, colour, gender, sex, sexual orientation, national origin, veteran status, disability, ancestry, or age.

11.3.4.2 Send, receive, solicit, print, copy, or reply to messages that are disparaging or defamatory.

11.3.4.3 Spread gossip, rumours, or innuendos about agents, employees, clients, suppliers, or other outside parties.

11.3.4.4 Send, receive, solicit, print, copy, or reply to sexually oriented messages or images.

11.3.4.5 Send, receive, solicit, print, copy, or reply to messages or images that contain foul, obscene, disrespectful, or adult-oriented language.

11.3.4.6 Send, receive, solicit, print, copy, or reply to messages or images that are intended to alarm others, embarrass our agency, negatively impact productivity, or harm morale.

11.3.5 The purpose of these rules is to ensure that information sent or received via our agency's IT systems is appropriately protected, that these systems do not introduce undue security risks to our agency and that users are made aware of what our agency deems as acceptable and unacceptable use of its email and IM.

11.3.6 Our agency has implemented an Internal Devices, Internet And Email Usage Policy in order to set out rules for our agents and employees to follow and to create the necessary framework and accountability in the event of misuse or negligence.

11.4 Our agency's rules related to handheld devices

11.4.1 Many users are unaware that mobile devices represent a threat to IT and data security.

11.4.2 As a result, they often do not apply the same level of security and data protection as they would on other devices such as their own desktop or laptop computers.

11.4.3 Our agency accepts that, with the rapid advancement of technology, our agents and employees would inevitably make use of smart phones and tablets with phone capability in addition to their agency issued laptops.

11.4.4 These would be personal devices or as provided by the agency based upon eligibility as per designation and to assist agile decision making, provide visibility to data, statistics, and reports; while on the move through the personal devices or agency provided devices.

11.4.5 However, information security essentials need to be integrated into all such personal devices if agency information will be available on these personal devices. The rationale is to provide speed of communication and facile access to business requirement while user is on the move.

11.4.6 Our agency does however recognize that the use of these facilities within and out of office premises poses various risks.

11.4.7 Our agency has implemented internal rules related to the corporate usage of personal devices, within the Internal Devices, Email And Internet Usage Policy which shall address the risks associated with:

11.4.7.1 Loss, disclosure, corruption or manipulation of corporate data on personally owned devices;

11.4.7.2 Incidents involving threats to, or compromise of, the agency's IT infrastructure and other information assets (e.g. malware infection or hacking);

11.4.7.3 Non-compliance with applicable laws, regulations and obligations (e.g. privacy or piracy);

11.4.7.4 Intellectual property rights for corporate information created, stored, processed or communicated on these devices in the course of work.

11.4.8 Management of the agency reserves the right not to authorize individuals, or to withdraw the authorization, if they deem the personal device not to be appropriate and in the best interests of the agency.

11.4.9 Our agency safeguards the physical and data security of mobile devices such as smartphones, tablets, and other mobile devices like PC's and Notebooks and our agency's Information Officer and the IT department ensures that:

11.4.9.1 Our agency's users of handheld devices diligently protect their devices from loss and disclosure of private information belonging to or maintained by our agency and that this is achieved with constant awareness training.

11.4.9.2 Before connecting a mobile handheld device to the network at our agency, users are expected to ensure it is on the list of approved devices issued by the IT support wherever necessary.

11.4.9.3 In the event of a security incident or if suspicion exists that the security of our agency's systems has been breached, the person in our agency who becomes aware of the breach shall notify the IT support team immediately together with our agency's Information Officer especially when a mobile device may have been lost or stolen.

11.4.10 Basic minimum standards of safety, as mentioned by the product vendor, should always be adhered to.

11.4.11 Business equipment should always be safeguarded against natural and manmade disasters, pests, power failures etc.

11.4.12 All supporting utilities (such as power supply, water supply, heating/ ventilation, air conditioning) shall be adequate for the systems they support.

11.4.13 The following should be ensured as part of cabling security:

11.4.13.1 All cables, including power and telecommunication network cables, shall be protected from damage or unauthorized interception;

11.4.13.2 Documents, such as detailed physical network diagrams, showing cable routings and terminations shall be maintained by the Administration department;

11.4.13.3 As far as possible, power and communication cables shall be segregated;

11.4.13.4 Network cables shall be protected from unauthorized interception or damage due to environmental hazards.

11.4.14 The siting of the equipment should ensure that routine and emergency maintenance of the equipment should be possible to be carried out effectively. Such maintenance should be carried out in accordance with the supplier's recommended service intervals and specifications.

11.4.15 Movements of equipment should be tracked.

11.4.16 Adequate contacts with other authorities including utilities, emergency services, health and safety departments, should be in place.

11.4.17 Decommissioning / disposal of IT and non-IT equipment should be done, and measures should be deployed to ensure that no advertent or inadvertent loss of data / violation of any regulatory compliance take place.

11.5 Tracking Technologies and Cookies

11.5.1 Cookies and similar tracking technologies are used to track the activity on our agency's website and to store certain information.

11.5.2 Tracking technologies our website may use include beacons, tags, and scripts to collect and track information and to improve and analyse the efficiency of the website. The technologies which may be used to track information may include:

11.5.2.1 Cookies or Browser Cookies. A cookie is a small file which may be placed on a data subject's device. Data subjects can instruct their browser to refuse all Cookies or to indicate when a Cookie is being sent. However, if this function of our website is not accepted, data subjects may not be able to use some parts of the website. Unless the browser settings have been adjusted, our website may use Cookies.

11.5.2.2 Local Storage and Similar Technologies. Certain features of the website may use browser local storage, session storage or similar technologies to collect and store information about data subjects' preferences or activity on the website. These are not always managed by the same browser settings as those used for Browser Cookies, and data subjects who wish to clear this information should refer to their browser's privacy or site-data settings.

11.5.2.3 Web Beacons. Certain Sections of the website and emails may contain small electronic files known as web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) that permit our agency access for example, to count users who have visited those pages or opened an email and for other related website statistics (for example, recording the popularity of a certain Section and verifying system and server integrity).

11.5.3 Cookies can be “Persistent” or “Session” Cookies. Persistent Cookies remain on data subjects' personal computer or mobile device even when offline, while Session Cookies are deleted as soon as data subjects' web browsers are closed.

11.6 Physical access control

11.6.1 All of our agency's premises that include computers and other types of information technology resources will be safeguarded against unlawful and unauthorized physical intrusion, as well as fire, flood and other physical threats.

11.6.2 This includes but is not limited to; security doors, key entry areas, external doors that are locked from closing until opening of the building, locked and/or barred windows, security cameras, registration of visitors at entrances, security guards, and fire protection.

12. THIRD PARTY OPERATORS

12.1 Where necessary for our legitimate business operations, contractual obligations or legal requirements, our agency may disclose data subjects' personal and, in limited circumstances, special personal information to third-party service providers ('operators') for specific reasons related to our service delivery.

12.2 Operators (i.e. third parties which may process personal information on behalf of our agency) include call centres, outsourced payroll administrators, marketing database companies, recruitment agencies, psychometric assessment centres, document management warehouses, external consultants and software providers.

12.3 Our agency will implement the following key obligations in respect of operators:

12.3.1 The operator may not process personal information on behalf of our agency without the knowledge and authorisation of our agency;

12.3.2 Our agency will ensure that the operator implements the security measures required in terms of our Data Privacy Terms and Conditions;

12.3.3 There will be a written contract in place between our agency and the operator, the Third-Party Operator's Non-Disclosure AGREEMENT which requires the operator to maintain the confidentiality and integrity of personal information processed on behalf of our agency; and

12.3.4 If the third party is located outside of South Africa, our agency will comply with the requirements in POPIA (including Section 72) in respect of transborder transfers of personal information.

12.4 If our agency (or an operator processing personal information on its behalf) becomes aware of a security compromise involving personal information, or has reasonable grounds to believe that such a compromise has occurred, it will notify the Information Regulator via the Regulator's eServices Portal, and the relevant data subjects (if their contact details are available), as soon as reasonably possible in accordance with Section 22 of POPIA and clause 15.8 below. This notification obligation applies irrespective of the perceived level of risk, consistent with clause 15.8.3.

12.5 As referenced in clauses 1 to 7 above, where necessary we will obtain Consent from the particular data subject.

12.6 These OPERATORS' AGREEMENTS are necessary in order to ensure that the third-party operator treats the personal information of our agency's data subjects responsibly and in accordance with the provisions contained in POPIA and Regulations thereto.

12.7 When we present our OPERATORS' AGREEMENTS to a third-party for signature, we usually request copies of the third-party operators' POPIA Policy, rules, internet rules and details of the third-party's Information Officer.

13. BANKING DETAILS

13.1 It is a known fact that South African businesses are particular targets for email interceptions and in particular the interception of banking details for purposes of payment in respect of transactions.

13.2 Our data subjects are open to large amounts of damages and losses if emails are intercepted, and banking details are fraudulently amended without the data subject's knowledge.

13.3 We have implemented an Internal Payments Policy which has been circulated to all agents and employees and in accordance with which our agents and employees are formally held liable when not following our rules as well as clear warnings within all our correspondences (emails and physical letters) warning data subjects of the risks of email hacking and interceptions.

13.4 In the event that banking details are sent to data subjects or received from data subjects for purposes of payment, the banking details will be sent via a secure channel (other than email) and must be confirmed with a telephone call and a follow up WhatsApp.

13.5 It is recorded that, in certain instances, data subjects' bank details are to be shared with relevant third parties but in such event, all care shall be taken to ensure encryption of emails.

14. DIRECT MARKETING

14.1 Our agency does not share data subjects' information with third-parties for the sole purpose of using the information for direct marketing.

14.2 Our agency may approach existing clients using their Personal Information for the purposes of direct electronic marketing of our own similar property and related real estate services, provided the client's details were obtained in the context of a sale or the provision of our services, and the client was given a reasonable opportunity, free of charge and without unnecessary formality, to object to such use both at the time the information was collected and on the occasion of each subsequent communication, in accordance with Section 69(3) of POPIA.

14.3 We will always ensure that the required OPTING OUT/UNSUBSCRIBE options which allow the recipients of marketing communications to request a removal of their details from our marketing communications are clearly implemented in every communication, together with the identity of the agency as sender.

14.4 Management of our agency will, from time to time, send necessary information to the agency's client base and to this end, the members will discuss and update the agency's direct marketing strategies.

14.5 We may utilise the Personal Information of an existing client of the agency for the purposes of providing our client with information regarding property and related real estate services that may be of interest to the client (direct electronic marketing).

14.6 New clients of the agency must be given an opportunity to object to receiving direct marketing material by electronic communication at the time that their personal information was collected.

14.7 Our agency may only approach a person who is not an existing client using their Personal Information for direct electronic marketing purposes if we have obtained that person's prior, opt-in Consent to do so, in compliance with the Information Regulator's Guidance Note on Direct Marketing (December 2024) and the POPIA Amendment Regulations, 2025.

14.8 The agency may only carry out direct marketing (using any form of electronic communication, including telephone calls, which the Information Regulator treats as electronic communications for this purpose) to non-clients if we have received their Consent to do so. Pre-ticked consent boxes, an assumed opt-in, or silence do not constitute valid Consent. Where Consent is obtained telephonically, the call will be recorded, the recording will reference the goods or services being marketed and the method of communication (mirroring the content of Form 4 of the Regulations, being the prescribed form for Consent to direct marketing), and the recording will be retained and made available to the data subject on request.

14.9 Our agency may approach a person to ask for their Consent to receive direct marketing material only once, and we may not do so if they have previously refused their Consent.

14.10 Should our agency receive Consent to send direct electronic marketing to a non-client of the agency, such direct electronic marketing material must have an opt-out option and must clearly identify our agency as the sender.

14.11 If you currently receive marketing information from us which you would prefer not to receive in the future, please email us at margie@capewaterfrontestates.co.za.

14.12 Our agency does not make “cold calls” using unsolicited telephone marketing without prior Consent, and our number should not appear on our data subjects' devices as “spam”.

15. INFORMATION OFFICER

15.1 Our agency's appointed Information Officer is:

MARGIE ANN MACKENZIE

Postal address: 43 Victoria Avenue, Hout Bay, 7806

Registered address: 43 Victoria Avenue, Hout Bay, 7806

Physical Address: 43 Victoria Avenue, Hout Bay, 7806

Tel: 021 790 7644

Email: margie@capewaterfrontestates.co.za

15.2 Our Information Officer is duly appointed by Management of our agency and both the agency, and the Information Officer are duly registered on the Information Regulator's eServices Portal.

15.3 In fulfilling her duties, the agency's Information Officer refers to the Information Regulator's Guidance Notes in order to ensure that she fulfils her duties as required in terms of Section 55 of POPIA.

15.4 The general responsibilities of our agency's Information Officer include the following:

15.4.1 To ensure that a compliance framework is developed, implemented, monitored, continuously reviewed and improved;

15.4.2 To ensure that a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;

15.4.3 That a Manual is developed, monitored, maintained and made available as prescribed in Sections 14 and 51 of PAIA, as amended;

15.4.4 That internal measures are developed together with adequate systems to process requests for information or access thereto;

15.4.5 That internal awareness sessions are conducted regarding the provisions of POPIA, regulations made in terms of POPIA, codes of conduct, or information obtained from the Regulator;

15.4.6 That, upon request by any person, copies of the manual are provided to that person upon the payment of a fee to be determined by the Regulator from time to time;

15.4.7 To ensure that the Incident Response Policy is circulated to all agents and employees and that data incidents are properly managed when they occur, including reporting via the Information Regulator's eServices Portal;

15.4.8 To encourage compliance, by all agents and employees with the conditions for the lawful processing of personal information;

15.4.9 To work with the Regulator in relation to investigations conducted pursuant to prior authorisation required to process certain information of POPIA in relation to the agency;

15.4.10 To ensure continuous data backups and test those backups regularly for data integrity and reliability;

15.4.11 To review Policy rules regularly, document the results, and update the Policy as needed;

15.4.12 To continuously update information security policies and network diagrams;

15.4.13 To ensure that critical operational applications and data are secure by patching known vulnerabilities with the latest fixes or software updates; and

15.4.14 To perform continuous computer vulnerability assessments and audits.

15.5 Registration of Information Officers with the Regulator is not only the prerequisite for an Information Officer to take up their duties in terms of POPIA but is a compulsory requirement for every person identified and appointed by the agency as Information Officer.

15.6 Annual filing requirements:

15.6.1 The Information Officer must annually, in terms of Section 32 of PAIA, submit to the Regulator a report regarding:

15.6.1.1 The number of requests for access received; the number of requests for access granted in full; the number of requests for access granted in terms of Section 46 of PAIA;

15.6.1.2 The number of requests for access refused in full and refused partially and the number of times each provision of PAIA was relied on to refuse access in full or partially;

15.6.1.3 The number of cases in which the periods stipulated in Section 25(1) of PAIA were extended in terms of Section 26 (1) of PAIA;

15.6.1.4 The number of internal appeals lodged with the relevant authority and the number of cases in which, as a result of an internal appeal, access was given to a record;

15.6.1.5 The number of internal appeals which were lodged on the ground that a request for access was regarded as having been refused in terms of Section 27 of PAIA;

15.6.1.6 The number of applications to a court which were lodged on the ground that an internal appeal was regarded as having been dismissed in terms of Section 77(7) of PAIA.

15.6.2 The Regulator may, annually, request an Information Officer of a private body, in terms of Section 83(4) of PAIA, to furnish to the Regulator with information about requests for access to records of that body.

15.7 Delegation of duties to a Deputy Information Officer:

15.7.1 An Information Officer(s) of both a public or private body may, subject to legislation and policies governing the employment of personnel of the body concerned, delegate any power or duty conferred or imposed on him or her to a Deputy Information Officer of that body in terms of Section 56(b) of POPIA and Section 17(3) of PAIA;

15.7.2 Only an agent or employee of a body can be delegated as a Deputy Information Officer;

15.7.3 At the time of drafting these terms and conditions, the agency had not formally appointed a Deputy Information Officer, and these clauses are inserted herein for purposes of future reference when and if the agency appoints such a Deputy;

15.7.4 The delegation referred to above must be in writing, using the template provided in the Information Regulator's Guideline;

15.7.5 The delegation of any powers or duties and responsibilities to a Deputy Information Officer does not prohibit an Information Officer from exercising the powers or performing the duty that he or she has delegated to a Deputy Information Officer;

15.7.6 Any power, duties and responsibilities delegated to a Deputy Information Officer should be exercised or performed subject to such conditions as an Information Officer may consider necessary;

15.7.7 Any conditions of delegation, as conferred on the Deputy Information Officer, should ensure that the body is as accessible as reasonably possible for data subjects or requesters;

15.7.8 An Information Officer of a body must ensure that he or she reserves his or her rights in the aforesaid delegation to exercise the powers or to perform the duties and responsibilities concerned himself or herself; and withdraw or amend the aforesaid delegation at any time;

15.7.9 An Information Officer must be aware that any right or privilege acquired, or any obligation or liability incurred as a result of a delegation of any powers, duties and responsibilities is not affected by any subsequent withdrawal or amendment of the decision to delegate;

15.7.10 Depending on the circumstances of the case, the obligation or liability incurred as a result of any delegation of any powers, duties and responsibilities may be imposed on either the Information Officer or our agency in so far as POPIA is concerned in line with Section 17(6)(b) of PAIA;

15.7.11 To ensure a level of accountability by a delegated Deputy Information Officer, bodies are encouraged to ensure that such duties and responsibilities or any power delegated to a Deputy Information Officer is part of his or her job description;

15.7.12 Despite the above-mentioned delegation of a Deputy Information Officer, an Information Officer retains the accountability and responsibility for the functions delegated to the Deputy Information Officer;

15.7.13 To ensure accessibility of the body, the Deputy Information Officer(s) of a multinational entity must be based within the Republic.

15.8 The data breach responsibilities of our agency's Information Officer include the following:

15.8.1 Ascertaining whether personal data was breached;

15.8.2 Assessing the scope and impact by referring to the following:

15.8.2.1 Estimated number of data subjects whose personal data was possibly breached;

15.8.2.2 Determining the possible types of personal data that were breached; and

15.8.2.3 Listing the security measures that were already in place to prevent the breach from happening.

15.8.3 In accordance with Section 22 of POPIA, our agency will notify the parties listed below as soon as reasonably possible after becoming aware of reasonable grounds to believe that a compromise has occurred, via the Information Regulator's eServices Portal. This notification obligation is not subject to a risk threshold – our agency will notify the Information Regulator of every security compromise involving personal information, irrespective of the perceived level of risk, and the assessment described in clause 15.8.2 above informs the content of that notification rather than whether it is given:

15.8.3.1 The Information Regulator; and

15.8.3.2 Any data subject of the agency who may require notification, unless notification would impede a law enforcement investigation.

15.8.4 Communication should include the following:

15.8.4.1 Contact details of Information Officer;

15.8.4.2 Details of the breach;

15.8.4.3 Likely impact;

15.8.4.4 Actions already in place, and those being initiated to minimise the impact of the data breach; and

15.8.4.5 Any further impact is being investigated (if required), and necessary actions to mitigate the impact are being taken.

15.9 Review and monitor

15.9.1 Once the personal data breach has been contained, our agency will conduct a review of existing measures in place and explore the possible ways in which these measures can be strengthened to prevent a similar breach from reoccurring.

15.9.2 All such identified measures should be monitored to ensure that the measures are satisfactorily implemented.

16. GDPR AND OTHER DATA PROTECTION LAWS

16.1 Our agency's primary data protection obligations, and the obligations described throughout this Policy, arise under POPIA and other applicable South African legislation.

16.2 Our agency does not target or offer its real estate services to individuals in the European Union or European Economic Area (EU/EEA), and does not consider itself subject to the EU General Data Protection Regulation (GDPR) on that basis. The mere fact that a website can be viewed by a person located in the EU/EEA does not, by itself, bring a South African business within the scope of the GDPR; broadly, the GDPR applies to organisations established in the EU/EEA, and to organisations outside the EU/EEA that specifically offer goods or services to, or monitor the behaviour of, individuals located in the EU/EEA.

16.3 Where any other data protection legislation does apply to a particular processing activity of our agency (for example, because a client or supplier is based abroad and that country's law has extraterritorial effect), our agency will take reasonable steps to comply with the applicable requirements of that legislation in respect of that activity, in addition to our obligations under POPIA.

17. AVAILABILITY AND REVISION

17.1 A copy of this public-facing Policy, excluding internal security schedules and disaster recovery materials, is made available on our agency's website www.capewaterfrontestates.co.za, from our agency's Information Officer at margie@capewaterfrontestates.co.za, and at our Hout Bay office.

17.2 This Policy will continually be updated to comply with legislation, including amendments to POPIA, its Regulations and guidance issued by the Information Regulator, thereby ensuring that personal information will remain secure.

ANNEXURE B

THESE FORMS ARE TO BE DIGITISED AND PUBLISHED ON THE AGENCY'S WEBSITE ALONGSIDE THIS POLICY

These forms reflect the Regulations Relating to the Protection of Personal Information, 2018, as amended by the Information Regulator's Amendment Regulations, 2025 (in effect 17 April 2025). Under the current numbering, Form 1 is for objections to processing, Form 2 is for correction/deletion requests, Form 3 is an application for the issuing of a Code of Conduct (not reproduced here, as it is not used by data subjects), Form 4 is the Consent form for direct marketing (reproduced below), and Form 5 is used to lodge a complaint with the Information Regulator (see clause 10.13 of this Policy). The current official templates are published by the Information Regulator at

https://inforegulator.org.za

REGULATED FORM 1

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

Regulations Relating to the Protection of Personal Information, 2018 (as amended, 2025) [Regulation 2]

Note: (1) Affidavits or other documentary evidence as applicable in support of the objection may be attached. (2) If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page. (3) Complete as applicable. This request is processed free of charge.

A DETAILS OF DATA SUBJECT	
Name and surname of data subject	
Residential, postal or business address	
Contact number(s)	
Fax number	
E-mail address	

B DETAILS OF RESPONSIBLE PARTY	
Name and surname of responsible party (if a natural person)	
Residential, postal or business address	
Contact number(s)	
Fax number / E-mail address	

C REASONS FOR OBJECTION (please provide detailed reasons for the objection)

Signed at _____ this _____ day of _____ 20____

_____

Signature of data subject (applicant)

REGULATED FORM 2

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

Regulations Relating to the Protection of Personal Information, 2018 (as amended, 2025) [Regulation 3]

Note: (1) Affidavits or other documentary evidence as applicable in support of the request may be attached. (2) If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page. (3) Mark the appropriate box: correction/deletion of personal information, or destroying/deletion of a record. This request is processed free of charge and must be responded to in writing within 30 days.

A DETAILS OF THE DATA SUBJECT	
Surname	
Full names	
Identity number	
Residential, postal or business address	
Contact number(s)	
Fax number	
E-mail address	

B DETAILS OF RESPONSIBLE PARTY	
Name and surname of responsible party (if a natural person)	
Residential, postal or business address	
Contact number(s)	
Fax number / E-mail address	

C REASONS FOR THE CORRECTION OR DELETION OF THE PERSONAL INFORMATION, OR DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT (please provide detailed reasons for the request)

Signed at _____ this _____ day of _____ 20____

_____

Signature of data subject (applicant)

REGULATED FORM 4

APPLICATION FOR THE CONSENT OF A DATA SUBJECT FOR THE PROCESSING OF PERSONAL INFORMATION FOR THE PURPOSE OF DIRECT MARKETING IN TERMS OF SECTION 69(2) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

Regulations Relating to the Protection of Personal Information, 2018 (as amended, 2025) [Regulation 6]

Note: Consent must be an unambiguous, opt-in action. Pre-ticked boxes and silence are not valid Consent. Where Consent is given telephonically, the call is recorded and the recording retained and made available to the data subject on request.

A DETAILS OF THE DATA SUBJECT	
Name(s) and surname / registered name of data subject	
Unique identifier/Identity number	
Residential, postal or business address	
Contact number(s)	
Fax number/E-mail address	

B DETAILS OF RESPONSIBLE PARTY	
Name(s) and surname/ registered name of responsible party or designated person	
Unique identifier/Identity number	
Residential, postal or business address	
Contact number(s)	
Fax number/E-mail address	

C GOODS OR SERVICES (specify goods or services being marketed):

_____

D MARKETING METHOD (specify marketing method, i.e. email, SMS, WhatsApp, telephone):

_____

My signature below confirms that I have consented to receive direct marketing pertaining to the goods or services specified above by the means of the marketing method specified.

Signed at _____ this _____ day of _____ 20____

_____

Signature of data subject/designated person

DEFINITIONS

1. **"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;
2. **"Child":** means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself;
3. **"Competent person":** means any person who is legally competent to Consent to any action or decision being taken in respect of a matter concerning a child;
4. **"Consent":** means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information, given through a clear affirmative action; pre-ticked boxes, silence or inaction do not constitute Consent;
5. **"Data subject":** means the person to whom personal information relates and for the purposes of our agency, this will include but not be limited to our clients, employees, external service suppliers and all associates of our agency;
6. **"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 of our agency, our real estate services to the data subject; or b) Requesting the data subject to make a donation of any kind for any reason;
7. **"Electronic communication":** means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient, and includes, for purposes of direct marketing, a telephone call;
8. **"eServices Portal":** means the Information Regulator's online portal used for the registration of Information Officers, the lodging of complaints, and the notification of security compromises;
9. **"Filing system":** means any structured set of personal information which in the case of our agency consists of physical files kept in the offices of our agency together with the data filed on the various software systems used by our agency;
10. **"IDSS":** means the agency's authorised Internet and Digital Services Suppliers, details of which are maintained in the agency's internal Cyber Security Measures schedule;
11. **"Operator":** means a person or entity who processes personal information for our agency in terms of a contract or mandate, without coming under the direct authority of our agency;
12. **"Our agency":** for purposes of these Data Privacy Terms and Conditions means:

BUSINESS NAME	CAPE WATERFRONT ESTATES CLOSE CORPORATION
REGISTRATION NUMBER	CK 94/11478/23
BUSINESS ADDRESS	43 VICTORIA AVENUE, HOUT BAY, 7806

with all agents, administrators and employees in our agency, whether permanent or temporary, who constitute the agency included insofar as their obligations are concerned and contained in this Policy and all other Data Privacy Policies associated with this Policy.

13. **"Person":** means a natural person or a juristic person;

14. **"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: information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, e-mail address, telephone number, location information, online identifier or other particular assignment to the person; the biometric information of the person; the personal opinions, views or preferences of the person; correspondence sent by the person that would reveal the contents of the original correspondence if the message is of a personal or confidential nature; the views or opinions of another individual about the person; and 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;

15. "Private body" means—

    15.1 a natural person who carries or has carried on any trade, business or profession, but only in such capacity;

    15.2 a partnership which carries or has carried on any trade, business or profession; or

    15.3 any former or existing juristic person, but excludes a public body

16. "Processing": means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including–

    16.1 The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

    16.2 Dissemination by means of transmission, distribution or making available in any other form; or

    16.3 Merging, linking, as well as restriction, degradation, erasure or destruction of information;

17. **"Promotion of Access to Information Act":** means the Promotion of Access to Information Act (PAIA), 2000 (Act No. 2 of 2000), as amended;

18. **"Public record":** means a record that is accessible in the public domain, and which is in the possession of or under the control of a public body, whether or not it was created by that public body.

19. **"Record":** means any recorded information –

    19.1 Regardless of form or medium, including any of the following: I. Writing on any material; II. 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; III. Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; IV. Book, map, plan, graph, or drawing; V. Photograph, film, negative, tape or other device in which one or more visuals images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;

    19.2 In the possession or under the control of our agency; and

19.3 Regardless of when it came into existence;

20. **"Regulator":** means the Information Regulator established in terms of Section 39 of the POPIA;

21. **"Responsible party":** means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information and, for purposes of this Policy, means our agency;

22. **"Restriction":** means to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information;

23. **"Special personal information":** means personal information as referred to in Section 26 of the POPIA which includes information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

24. **"This Act":** means the Protection of Personal Information Act, No. 4 of 2013, as amended;

25. **"Unique identifier":** means any identifier that is assigned to a data subject and is used by our agency for the purposes of the operations of our agency and that uniquely identifies that data subject in relation to our agency.

cape waterfront
estates

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013
DATA PRIVACY TERMS AND CONDITIONS
2026

IMPLEMENTATION RESOLUTION

DATE OF ADOPTION: 7.9.26

1. Management of our agency acknowledges the need to analyse and mitigate the wide variety of risks to which the agency is exposed and has put together the Data Privacy Terms and Conditions in order to mitigate the cyber and data-protection risks associated with the agency's operations, to align with the Information Regulator's Amendment Regulations, 2025, and to enhance the agency's crisis and disaster mitigation measures in the event of these risks occurring.

To this end, Management of the agency resolves that:

2. These Data Privacy Terms and Conditions are implemented on signatures hereto;
3. These Data Privacy Terms and Conditions shall be circulated to all employees within 30 days after implementation;
4. Training for employees will be arranged within 60 days after implementation;
5. The IT department shall continue to be engaged with regard to the data security risks.

MEMBERS	SIGNATURE AND DATE
MARGIE ANN MACKENZIE	7/9/26
CLARE ELAINE PUTSMAN	7/9/26