



Camelot Wealth

(Pty)Ltd | FSP 54863 | Reg 2024/016417/07

Protection of Personal Information (POPI) Policy

1. Introduction

Camelot Wealth (Pty) Ltd (“the Company”) is committed to protecting the confidentiality, integrity, and security of personal information in compliance with the Protection of Personal Information Act, 2013 (POPIA) and related regulations.

The Company recognises that lawful and responsible processing of personal information is essential to maintaining trust, complying with FSCA requirements, and delivering quality financial services.

2. Purpose of Policy

This policy aims to:

- Ensure that all personal information is processed lawfully, fairly, and transparently.
 - Define how personal information is collected, used, stored, shared, and destroyed.
 - Protect the privacy rights of clients, employees, and third parties.
 - Set out responsibilities of employees and representatives in handling personal information.
-

3. Scope

This policy applies to:

- All directors, employees, representatives, contractors, and service providers of Camelot Wealth.
 - All personal information processed by the Company relating to clients, staff, product suppliers, and third parties.
-

4. Definition of Personal Information

Personal information means information relating to an identifiable living natural person or juristic person, including but not limited to: names, identity numbers, contact details, financial records, policy details, health information, and correspondence.

5. POPIA Principles (Conditions for Lawful Processing)

The Company adheres to the following eight conditions under POPIA:

1. Accountability – The Company ensures compliance through its appointed Information Officer.
2. Processing Limitation – Only necessary and lawful personal information is collected.
3. Purpose Specification – Data is collected for clear, legitimate business purposes.
4. Further Processing Limitation – Data is not processed beyond the original purpose unless required by law or with consent.
5. Information Quality – Data is accurate, complete, and updated regularly.
6. Openness – Clients are informed of what data is collected and why.
7. Security Safeguards – Technical and organisational measures are in place to protect information.
8. Data Subject Participation – Clients have rights to access, correct, or request deletion of their personal information.

6. Information Officer

- The Board has appointed an Information Officer in terms of POPIA.
- The Information Officer is responsible for monitoring compliance, responding to requests, reporting breaches, and maintaining POPIA documentation.

7. Processing of Personal Information

7.1 Collection

- Information is collected directly from clients (via application forms, correspondence, meetings) or lawfully from third parties (e.g., product providers).
- Only necessary information is requested for business and regulatory purposes.

7.2 Use

- Information is used strictly for providing financial services, product administration, compliance reporting, and communication with clients.

7.3 Storage

- Physical documents are stored in locked cabinets with controlled access.
- Electronic data is stored on password-protected systems with encryption and regular backups.

7.4 Sharing

- Information is shared only where required for financial services, with authorised third parties (e.g., product providers, regulators), and with client consent.

7.5 Retention & Destruction

- Records are retained in line with FSCA/FAIS requirements (minimum 5 years).
 - After expiry, information is securely destroyed (shredding for paper, certified deletion for digital).
-

8. Rights of Data Subjects

Clients and employees have the right to:

- Request access to their personal information.
 - Request correction or deletion of inaccurate or outdated information.
 - Withdraw consent where processing is based on consent.
 - Object to processing under certain circumstances.
 - Lodge complaints with the Information Regulator.
-

9. Security Safeguards

- Access controls and role-based restrictions.
 - Password policies and multi-factor authentication.
 - Firewalls, anti-virus software, and encryption.
 - Secure physical storage and shredding of hard copies.
 - Incident reporting and breach notification protocols.
-

10. Breach Management

- Any suspected data breach must be reported immediately to the Information Officer.
 - The Information Officer will investigate, mitigate, and, where necessary, notify the Information Regulator and affected clients as required by POPIA.
-

11. Training & Awareness

- All staff receive POPIA training on induction.
- Annual refresher training ensures continued awareness.
- Staff sign Confidentiality & POPIA Undertakings.

12. Monitoring & Compliance

- Compliance with this policy is monitored by the Information Officer and Compliance Officer.
- Internal audits may be conducted to test the effectiveness of controls.
- Reports are submitted to the Board annually.

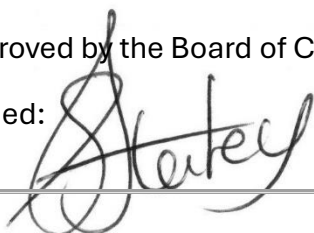
13. Review of Policy

This policy will be reviewed annually or when significant changes in law or business operations occur.

14. Approval

Approved by the Board of Camelot Wealth (Pty) Ltd.

Signed:



Director / Key Individual

Date: **20/02/2025**
