ANCHOR | NAVIGATING CHANGE

PROTECTION OF PERSONAL INFORMATION POLICY

THIS POLICY APPLIES TO:

Anchor Capital (Pty) Ltd	Erudite Financial Services (Pty) Ltd
Anchor Private Clients (Pty) Ltd	Nest Asset Management (Pty) Ltd
Anchor Financial Services (Pty) Ltd	Wild Dog (Pty) Ltd
Anchor Capital Investments (Pty) Ltd	ENI Financial Services (Pty) Ltd
Anchor Institutional (Pty) Ltd	Southridge Global Capital (Pty) Ltd
Anchor Stockbrokers (Pty) Ltd	Bryan Hirsch Colley and Associates (Pty) Ltd
Anchor Securities (Pty) Ltd	Retirement Planning Services (Pty) Ltd
Anchor Securities Private Clients (Pty) Ltd	Retirement Planning Services International (Pty) Ltd
Capricorn Fund Managers SA (Pty) Ltd	Robert Cowen Investments (Pty) Ltd
R Fisher and Associates (Pty) Ltd	

Hereinafter collectively referred to as "**Anchor**" or the responsible party.

CONTENTS

DEFINITIONS

Consent	Means any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of personal information.
Direct marketing	Means to approach a data subject, either in person, by mail, or electronic communication, for the direct or indirect purpose of: • Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or • Requesting the data subject to make a donation of any kind, for any reason.
Data subject(s)	Means the person to whom the personal information relates and can be a natural or legal/juristic person. It includes, but is not limited to, trusts, companies, closed corporations, and partnerships.
Operator	Means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.
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 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 the birth of that person; • information relating to the education or the medical, financial, criminal or employment history of the person; • any identifying number, symbol, e-mail address, physical 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 is implicitly, or explicitly, of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; • 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.
Processing	The act of processing information includes any activity or set of operations, whether by automatic means, concerning personal information and includes: • the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use; • dissemination by means of transmission, distribution or making available in any other form; or • merging, linking, as well as any restriction, degradation, erasure, or destruction of information.
Records	Means any recorded information, regardless of form or medium, including: Writing on any material; • 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; • a label, marking, or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; • book, map, plan, graph, or drawing; and • photograph, film, negative, tape, or other device in which one or more visual images are embodied to be capable, with or without the aid of some other equipment, of being reproduced.
Responsible party	Means each of the respective companies as listed in Annexure A, paragraph 1.
Unique Identifier	Means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

1. INTRODUCTION

The Protection of Personal Information Act 4 of 2013 (POPI) requires that Anchor Group (the responsible party) has plans and processes in place on how it processes, stores, and shares clients' personal information. The responsible party respects its clients' right to privacy and endeavours to collect and use their personal information minimally, transparently, and for the purpose for which such information was collected. This policy and its supporting documents are written in easily understandable language so that it is practical and usable to a wide audience in the business.

The responsible party is committed to keeping all information safe and secure, to provide persons with reasonable access to their personal information, and to give effect to their rights in terms of the POPI Act. To this extent, the responsible party emphasises that only necessary information is collected and used. The collection thereof serves to protect legitimate legal interests and ensures that the responsible party is able to offer its clients a service or product/s.

2. APPLICATION OF THIS POLICY

The obligations in this policy apply to the responsible party, its subsidiaries, associated entities, management, staff members, and representatives. Any third parties to whom the responsible party entrusts personal information are also bound by the respective terms as set out in this policy that references third-party operator management. This policy further applies to all personal information gathered from data subjects.

3. SECURITY MEASURES WITH REGARDS TO CONFIDENTIALITY OF PERSONAL INFORMATION

3.1. The purpose of collection

The responsible party requires certain categories of information to ensure that clients receive high-quality service and that their needs are met as they may require from time to time. The same goes for any partnerships, due diligence, or other third-party interactions, where personal information is gathered. Information may be collected for explicitly defined purposes or incidental to the function, activity, or service of the responsible party or a third party that might be one of the responsible party's service providers. Processing might also be automatic where software systems are used.

The responsible party warrants that personal information will never be used for any reason that is not in line with what such information is collected for. Should the purpose for which the responsible party collects information not be specified in this clause, it will be communicated to the data subject in writing and agreed to in our interactions with the data subjects, which might include varied and different parties.

3.2. Consent

Any information that we collect from data subjects will be obtained with their consent. Consent may be obtained from data subjects during introductory meetings, through application forms, by electronic media, or ongoing interaction. It might also be via online website cookies or any other form of valid consent.

Where data subjects provide the responsible party with information, the need to do so willingly and voluntarily with the understanding that the responsible party requires the information to pursue both its clients' legitimate interests as well as its own.

To carry on business and to protect or facilitate data subjects' interests, the responsible party will require personal information from time to time and will treat it with the utmost confidentiality. Should a data subject at any time during the processing of their personal information object to same, they may withdraw their consent by furnishing the responsible party with reasonable notice and in the prescribed form attached. In such circumstances, the responsible party will give due consideration to the request and the requirements of POPI. The responsible party may cease to use, or disclose the data subject's personal information and may, subject to any statutory and contractual record-keeping requirements, also approve the destruction of such personal information.

3.3. Information the responsible party requires

The responsible party collects different categories of information from data subjects, depending on their needs and agreements with them. We do not collect information that is unnecessary or irrelevant for the purposes specified. We strive to collect only information that is necessary for us to deliver our services.

To the extent that the responsible party requires information from data subjects, it will generally collect the following information which includes but is not limited to:

- ***Information relating to the education or the medical, financial, criminal, or employment history of the person.***
- ***Any identifying number, symbol, email address, physical address, telephone number, location information, online***

identifier, or other particulars assigned to the person.

- *The biometric information of the person.*
- *The personal opinions, views, or preferences of the person.*
- *Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence.*
- *The views or opinions of another individual about the person.*
- *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.*
- *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 such person.*
- *Personal information concerning a child.*

Please bear in mind that this is not an exhaustive list, and the responsible party may, at times, require other information that is not contained herein. The responsible party will inform data subjects as to the information we collect from them whenever practicable, whether such information is voluntary or mandatory, and what the consequences are if the information (whether voluntary or mandatory) is not provided. Usually, if the information requested is not provided, we can only offer a limited service or no service at all.

3.4. Access to and integrity of information

The responsible party is committed to maintaining the integrity and accuracy of data subjects' information. To this extent, data subjects are reminded, via consent forms (or other methods) that they may request access to their information at any time and also request that the responsible party update or correct any information that may be outdated or incorrect.

The responsible party will take reasonable and routine steps to ensure that the information collected is up to date and accurate. Where information does not need to be updated to fulfil the purpose for which it was collected, such information will not be updated without the client's express request.

The responsible party provides for four categories of requestors for access to information:

- *A person requesting his or her own information.*
- *A person requesting information for, and on behalf of, another person.*
- *A person requesting information about another person.*
- *A public body that requests information which is in the public interest.*

Requestors must provide proof of identity and a power of attorney, where applicable, and complete the prescribed form as attached. The responsible party may request any other information to verify the requestor's identity.

3.5. Security of information and regular monitoring

The safety and confidentiality of a data subject's information are of paramount importance to the responsible party and its staff. To this extent, the responsible party is committed to preventing unauthorised access, damage, loss or destruction of personal information, by ensuring that industry-appropriate and adequate security measures are in place and regularly reviewed.
The responsible party does its best to identify risks both internally and externally, and to adapt accordingly it implements security systems with due regard to generally accepted information security practices.

3.6. Holding periods

Information which the responsible party collects on data subjects will not be held for longer than necessary or, if the purposes for which said information was collected has ultimately been fulfilled, or if the collected information has become obsolete.

Where no agreements, other laws, or terms of this policy apply, a record of personal information will be kept for one year after the information processing was completed, including usage for the specific purpose for which the information was originally collected.

The responsible party will destroy records of personal information as soon as reasonably practicable unless further retention is required by the laws mentioned above or is agreed to between the parties. Automatic deletion will occur in accordance with our IT policies and Record Retention Policy.

3.7. Information erasure

The responsible party will endeavour that information be destroyed, where reasonable, after its retention period has lapsed as set out in the Record Retention Policy.

Data subjects have the right to obtain the erasure of their personal data without any undue delay if:

- the information is no longer necessary for the specified purpose it was collected for; or
- where the data subject withdraws consent in terms of this policy; or

- if the collected personal information is inaccurate, irrelevant, excessive, or incomplete.

If data subjects prefer that the responsible party ceases processing their personal information instead of deleting it, reasonable notice may be given to this effect following which the responsible party will immediately stop processing the data subject's information.

Notice in terms of erasure must be provided in the prescribed format of forms attached to this policy.

3.8. Direct marketing

The responsible party will never process personal information for the purpose of direct marketing (or spam) unless data subjects:

- have consented to such processing; or
- had not previously refused consent; and if
- contact details were obtained in the context of providing data subjects with our services; and if
- they were given reasonable opportunity to object to direct marketing; or
- they were already a data subject.

4. SECURITY MEASURES REGARDING AN OPERATOR OR PERSON ACTING UNDER AUTHORITY

4.1. Disclosure of information

The responsible party staff are regularly reminded that they have a confidentiality obligation towards data subjects who hold a right to privacy under the Constitution of South Africa, and neither the responsible party nor its staff will disclose data subject information to a third party unless:

- it is required to do so by law; or
- the disclosure is necessary to enable the responsible party to perform its functions as per its clients' mandates; or
- when it is vital in protecting the rights of the responsible party.

4.2. Authority

If information is to be disclosed to a third party, the responsible party will ensure that the third party receiving such personal information is as committed to protecting your privacy and information as the responsible party is. This is done by obtaining a written undertaking and disclosure form from the third party, where the third party agrees to keep the information confidential and maintains the necessary security measures.

We disclose information to third parties such as highlighted below:

- ***The responsible party shares information with software service providers for a variety of reasons including to add value to its clients' experience and to ensure that it remains operationally able to provide its suite of services.***
- ***Other than the software providers, the responsible party also shares information with:***
  - ***Other financial services companies and product providers.***
  - ***Regulatory authorities.***
  - ***Outsourced compliance services.***
- ***A client's email is also used as a method of communication in all businesses.***

5. DATA BREACH MANAGEMENT

A data breach incident is an event that has caused, or can potentially cause, damage to the responsible party organisation's assets, reputation, and/or personnel, which includes its clients and any other personal information it processes, stores, or shares. A data breach can occur when there is an intrusion, compromise, and misuse of information by a party that does not have lawful access rights to the information that was compromised.

An information security incident includes, but is not restricted to, the following:

- The illegitimate use of the responsible party's systems for the processing, storage, or sharing of data by any person.
- The transfer of personal information to persons who are not entitled to receive such information.
- The loss or theft of personal and/or classified data and information via any means, for example, hacking or even attempted hacking.
- Unauthorised changes to personal information via the responsible party's system hardware or software.
- The unauthorised disruption or denial of service to the responsible party's system.

Where there are reasonable grounds to suspect that the personal information of a data subject has been breached (accessed, acquired, deleted, or damaged by an unauthorised third party), the responsible party will:

- Notify the data subject of such a breach in detail; and
- inform the information regulator as soon as reasonably possible after such a breach is discovered.

Data breach communication to the data subject can be done in one of the following methods:

- Mailed to the data subject's last known physical or postal address;
- sent via e-mail to the data subject's last known e-mail address;
- placed in a prominent position on the website of the responsible party;
- published in the news media; or
- as may be directed by the regulator.

The communication must include enough information so that the data subject can take protective measures and should include:

- A description of the possible consequences of the breach;
- a description of the measures that the responsible party intends to take, or has taken, to address the security breach;
- a recommendation regarding the measures to be taken by the data subject;
- to mitigate the possible adverse effects of the breach; and
- if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.

The information regulator's contact details are as follows:

Address:
JD HOUSE, 27 Stiemens Street, Braamfontein,
Johannesburg, 2001

General enquiries:
enquiries@inforegulator.org.za

Complaints:
PAIAComplaints@inforegulator.org.za
and POPIAComplaints@inforegulator.org.za

6. PROHIBITED DATA PROCESSING AND EXEMPTIONS

Due to the nature of the responsible party's business, it may from time to time obtain data that is prohibited to enable it to offer its services and to comply with the laws applicable to its business. As such, the responsible party aims to make use of the exemptions that the POPI Act provides in instances where the information is needed. The responsible party will obtain consent for this personal information, and it may include but is not limited to:

- ***The religious or philosophical beliefs, race, or ethnic origin, trade-union membership, political persuasion, health or sex life or biometric information of a data subject.***
- ***The criminal behaviour of a data subject to the extent that such information relates to:***
  - ***The alleged commission of any offence by a data subject; or***
  - ***Any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.***
  - ***Personal information concerning a child.***

7. INFORMATION OFFICERS

The responsible party's information officer is responsible for:

- ***Ensuring information policies are reviewed, monitored, up to date and sufficient.***
- ***Ensuring an impact assessment is done.***
- ***Ensuring the PAIA manual is developed, monitored, maintained and available, as prescribed (if applicable).***
- ***Handling complaints or requests made in terms of this policy.***
- ***Supporting this policy with relevant documentation.***
- ***Ensuring POPI training or awareness is conducted.***
- ***Backing up data.***
- ***Reporting incidents and allocating security responsibilities.***
- ***Any other relevant information-related duty or responsibility.***

There will be continual reporting on POPI to the risk and compliance committees by the compliance department as per its terms of reference that may be amended from time to time. Please refer to Annexure A for information officer details.

8. DEPUTY INFORMATION OFFICERS

The deputy information officer is responsible for:

- ***The encouragement of compliance, by the company with the conditions for the lawful processing of personal information.***
- ***Dealing with requests made to the company pursuant to this Act.***
- ***Working with the regulator regarding any investigations conducted in relation to the company.***
- ***Otherwise ensuring compliance by the company with the provisions of this Act, as may be prescribed.***
- ***Officers must take up their duties in terms of this Act only after the responsible party has registered them with the regulator.***

Please refer to Annexure A for deputy information officer details.

9. STAFF AND/OR OTHER CONTRACTORS

In terms of POPI, the responsible party's companies, staff or other contractors will never:

- Process private information without a lawful reason.
- Share private information with anyone that should not have access to the information.
- Process more information than what is needed.
- Process information in a manner that is insecure.
- Ignore a request by a data subject relating to their information.
- Obstruct the operation of the information regulator.

10. PERSONAL INFORMATION TRANSFERS OUTSIDE SOUTH AFRICA

Due to the pervasive and widespread use of cloud technology, emails, and the disappearance of national borders in the broader context of the digital age in which we live, it is accepted that the personal information of data subjects will almost always be transferred globally. It is not always possible to pinpoint exactly in which country the cloud service is hosted as this may change from time to time as data centres operate internationally in several countries. It may well be the case that personal information is transferred to multiple countries.

The use of these services is required to be able to operate as a business, to stay competitive, and to keep up to date with new digital technological innovations. The responsible party also requires the use of these services to be able to provide clients with its services.

For all data subjects, the responsible party will obtain consent to transfer their information across borders before it does so. The reasons or platforms the responsible party uses to transfer personal information across borders include, but are not limited to:

- ***Cloud services for data file storage such as Sharepoint, OneDrive, etc.***
- ***Cloud server services for email.***
- ***Financial service performance data reporting processors.***
- ***Newsletter service providers.***
- ***Proprietary software services and the client relationship management (CRM).***

11. PRESCRIBED FORMS RELATING TO THE PROCESSING OF PERSONAL INFORMATION

For data subjects to exercise their rights in terms of their information, the responsible party needs to abide by the law. In this context, there are certain prescribed POPI forms to be used when interacting with data subjects.
Please see attached the forms for general use – All available on the Information Regulator website https://inforegulator.org.za/popia-forms/.

- ***Form 1 - Objection to the processing of personal information.***
- ***Form 2 - Request for correction or deletion of personal information or destruction or deletion of record of personal information.***
- ***Form 4 - Request for data subject's consent to process personal information for direct marketing.***

12. POPI AWARENESS

The responsible party conducts POPI awareness sessions with all of its staff or other consultants or contractors via online training. All previously mentioned persons will be required to have completed the POPI awareness training.

From time to time, more in-depth POPI awareness sessions may be held with the information officers and deputy information officers.

ANNEXURE A -INFORMATION OFFICERS AND DEPUTY INFORMATION OFFICERS

Business	Information Officer	Contact Details	Deputy Information Officer (S)	Contact Details
Anchor Capital (Pty) Ltd	Omair Khan	Email: okhan@anchorcapital.co.za Telephone no: 011 591 0638 / 072 777 5338	Liza Maartens	Email: lmaartens@anchorsecurities.co.za Telephone no: 011 591 0611 / 084 831 3600
			Nicole Marnewick	Email: nmarnewick@anchorcapital.co.za Telephone no: 011 591 0635 / 083 727 8950
Anchor Private Clients (Pty) Ltd	Liza Maartens	Email: lmaartens@anchorsecurities.co.za Telephone no: 011 591 0611 / 084 831 3600	Ronel van Niekerk	Email: rvanniekerk@anchorsb.co.za Telephone no: 011 591 0663 / 083 442 7085
Anchor Financial Services (Pty) Ltd	Neil Brown	Email: nbrown@anchorfs.co.za Telephone no: 011 591 0627 / 082 922 3964	Dale Franklin	Email: dfranklin@anchorfs.co.za Telephone no: 082 450 5444
Anchor Capital Investments (Pty) Ltd	Andrew Haiden	Email: ahaiden@anchorcapital.co.za Telephone no: 011 591 0696 / 083 469 4939	Matthew Norwood- Young	Email: mnyoung@anchorcapital.co.za Telephone no: 011 591 0683 / 083 677 0575
			Lara Meyer	Email: lmeyer@anchorcapital.co.za Telephone no: 011 591 0677/ 073 170 4774
Anchor Institutional (Pty) Ltd	Dale Franklin	Email: dfranklin@anchorfs.co.za Telephone no: 011 591 0628/ 082 450 5444	Mark Saunders	Email: msaunders@anchorfs.co.za Telephone no: 011 591 0681 / 071 898 0572
Anchor Stockbrokers (Pty) Ltd	Liza Maartens	Email: lmaartens@anchorsecurities.co.za Telephone no: 011 591 0611 / 084 831 3600	Ronel van Niekerk	Email: rvanniekerk@anchorsb.co.za Telephone no: 011 591 0663 / 083 442 7085
Anchor Securities Private Clients (Pty) Ltd	Nicola McMurtry	Email: nicola@anchorspc.co.za Telephone no: 031 819 6408 / 082 562 7279	Paul Patterson	Email: paul@anchorspc.co.za Telephone no: 031 819 6412 / 083 659 0812
Capricorn Fund Managers (Pty) Ltd	Andrew Haiden	Email: ahaiden@anchorcapital.co.za Telephone no: 011 591 0696 / 083 469 4939	Hein Kok	Email: hkok@anchorcapital. co.za Telephone no: 011 591 0590/ 072 514 495
			Liam Hechter	Email: lhechter@anchorcapital.co.za
R Fisher and Associates (Pty) Ltd	Brendan Gace	Email: bgace@anchorcapital.co.za Telephone no: 011 591 0691 / 082 346 3854	Michael Sarris	Email: msarris@anchorcapital.co.za Telephone no: 011 591 0690 /082 568 3839

Business	Information Officer	Contact Details	Deputy Information Officer (S)	Contact Details
Erudite Financial Services (Pty) Ltd	Omair Khan	Email: okhan@anchorcapital.co.za Telephone no: 011 591 0638 / 072 777 5338	Brendan Gace	Email: bgace@anchorcapital.co.za Telephone no: 011 591 0691 / 082 346 3854
Nest Asset Management (Pty) Ltd	Dale Franklin	Email: dfranklin@anchorfs.co.za Telephone no: 011 591 0631/ 082 441 0447	Mark Saunders	Email: msaunders@anchorfs.co.za Telephone no: 011 591 0681 / 071 898 0572
Wild Dog Capital (Pty) Ltd	Andrew Haiden	Email: ahaiden@anchorcapital.co.za Telephone no: 011 591 0696 / 083 469 4939	Matthew Norwood-Young	Email: mnyoung@anchorcapital.co.za Telephone no: 011 591 0683 / 083 677 0575
			Lara Meyer	Email: lmeyer@anchorcapital.co.za Telephone no: 011 591 0677/ 073 170 4774
ENI Financial Service (Pty) Ltd	Harold Hopking	Email: hhopking@anchorcapital.co.za Telephone no: 021 401 8966/ 083 468 0724		
Southridge Global Capital (Pty) Ltd	Nick Dennis	Email: ndennis@anchorcapital.co.za Telephone no: 021 401 8973 / 083 268 4115		
Bryan Hirsch Colley and Associates	Mark Colley	Email: markc@bhca.co.za Telephone no: 011 268 6908 / 082 789 8003	Julia Wiegele	Email: juliaw@bhca.co.za Telephone no: 011 268 6908 /082 445 5235
Retirement Planning Services (Pty) Ltd	Ancia Van Der Mescht	Email: ancia@rps.co.za Telephone no: 021 946 3184	Hendré De Vries	Email: hendre@rps.co.za Telephone no: 021 946 3184 071 679 4057
Retirement Planning Services International (Pty) Ltd	Ancia Van Der Mescht	Email: ancia@rps.co.za Telephone no: 021 946 3184	Hendré De Vries	Email: hendre@rps.co.za Telephone no: 021 946 3184/ 071 679 4057
AIH Capital (Pty) Ltd	Charlene Nyembe	Email: charlene@awcainvest.co.za Telephone no: 011 026 7422 / 083 335 9788	Sindi Mabaso-Koyana	Email: sindi@awcainvest.co.za Telephone no: 011 027 7422
Robert Cowen Investments (Pty) Ltd	Di Haiden	Email: di@rcinv.co.za Telephone no: 011 591 0572	Christine Ulyate	Email: christine@rcinv.co.za Telephone no: 011 591 0569 / 084 583 7183
			Marieke de Kok	Email: marieke@rcinv.co.za Telephone no: 011 591 0575 / 072 430 0707