We act respectfully, doing the right thing for the right reason to ensure our clients are safe with us.

Fairheads is a leading independent administrator and service provider to the retirement fund and fiduciary industries in Southern Africa.

Our fiduciary heritage dates back to 1925 as one of the first trust companies in South Africa. Fairheads participated in the pioneering of umbrella trusts in the 1980's and later played a major role in bringing beneficiary funds into being in 2009.

Thousands of dependants, many of them vulnerable minors, depend on us for the safe management of funds left to them by loved ones. In this way we make a valuable contribution to the education, maintenance, advancement and well-being of children all over Southern Africa.

We never lose sight of this responsibility.

The Fairheads brand has been developed through a steadfast commitment to accountability, integrity, professionalism, responsibility and service excellence.

OUR COMMITMENT

Fairheads is committed to ensuring the protection of all personal information which the company holds. We are dedicated to safeguarding the personal information under our control and to maintaining a compliance system to ensure that the company meets its information security obligations.

Protection of Personal Information Act

COMPLIANCE STATEMENT

The Protection of Personal Information Act ("POPIA") is intended to promote the right to privacy as enshrined in the Constitution, while at the same time protect the flow of personal information and advance the right of access to personal information. The Act provides a person (data subject) with a degree of control over his or her personal information and applies to all public and private bodies that process personal information.

Fairheads is committed to the 8 Principles contained in the POPI Act and related privacy legislation including the right to privacy as enshrined in the Constitution. Our privacy policies and procedures are designed to ensure that:

- personal information is processed in a lawful and reasonable manner.
- information is only processed for a specific, clearly defined and lawful purpose.
- steps are taken to ensure that the client is aware of the purpose of collecting the personal information.
- ensure that the collection of the personal information is compatible with the intended purpose of collecting the information.
- the information remains complete, accurate and current.
- the client and the regulator (where applicable) are advised in writing that the organisation is collecting personal information and record the purpose of the collection.
- the security and integrity of the personal information that has been collected is protected.
- the data subject is involved directly in the process of collecting the personal information to ensure that the information obtained is clear, accurate and current.

Fairheads is committed to providing a compliant and consistent approach to the protection of information. The company has always been dedicated to providing a robust and effective information security environment which complies with POPIA and related information security legislation and industry best practice. Fairheads recognises its obligations in respect thereof and is constantly updating and expanding its information security compliance programmes to meet the requirements of information security legislation.

In accordance with the Promotion of Access to Information Act (PAIA) of 2000, the company has a **PAIA Manual** which provides guidelines to clients on how to exercise their rights to access to information.

Fairheads collects, stores and processes personal information (which may include special personal information) from clients that may be used in connection with the administration of benefits and other activities conducted by Fairheads from time to time in compliance with the 8 POPIA principles. The **Personal Information Privacy Statement** explains the types of information Fairheads collects, the purpose of the collection and how Fairheads uses, discloses, stores and protects that information.

Fairheads has engaged in ongoing information security risk identification, risk assessment, monitoring and reporting since 2013. Information security compliance audits are performed at least annually with risk control monitoring and reporting conducted quarterly.

Fairheads has a Document Management Policy in place which sets out governance standards for electronic, digital and hardcopy document management. This is to ensure that the company complies with data minimisation, data storage limitation and the lawful processing of information. The company has a Document Retention Process which includes cloud storage of electronic data. Regular due diligence is conducted on 3rd party document storage service providers.

Ongoing compliance awareness on information security is communicated via staff notices, compliance bulletins and staff bulletins. Staff are assessed annually on their information security competence, application and understanding of information security. Fairheads' accountability and governance measures are in place which include staff completion of Declarations annually in which they attest to their compliance with Compliance Policies.

Fairheads also has Information Asset, Information Security and Information Systems Policies in place. IT compliance standards are also monitored in accordance with the King IV Code of Governance.

Fairheads' policies and governance information may be requested from the **Compliance Officer**, Darlene Van Dieman at compliance@fairheads.com. Darlene is the Group's Information Officer. She is also appointed as the Information Officer of some of the funds which Fairheads Benefit Services administers.

Fairheads Benefit Services (Pty) Ltd, is a private body and defined as a **"Responsible Party"** in terms of the Protection of Personal Information Act ("POPIA"). As such, whether alone or in conjunction with the trustees of the trusts and beneficiary funds which it administers, the Responsible Party determines the purpose of and means for processing personal information in compliance with the Administration Agreements signed with the trustees of the funds.

All clients have access to their personal information free of charge and upon request from Fairheads as the administrator of trusts and beneficiary funds.

The Boards of Trustees of the various Funds under the administration of Fairheads Benefit Services have access to the information of the funds of which they are the trustees.

Fairheads Benefit Services reports to the Boards of Trustees of the funds which it administers in terms of the signed Administration Agreements. The Heads of Compliance and Internal Audit report to the Assurance, Risk and Compliance Committee ("ARC") and and also report to the various sub-committees of which they are members. POPIA Compliance is a standard Agenda Item of the ARC Committee and is reported on bi-monthly to the Compliance Committee.

Fairheads does not outsource any of its administration services to any third party.

Fairheads as the Responsible Party processes the personal information of its clients which includes the members of the funds. "Processing" includes any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

- 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 restriction, degradation, erasure or destruction of information.

Fairheads has done extensive work on the compliance requirements for both the Promotion of Access to Information Act and Protection of Personal Information Acts since 2013 to ensure its readiness for the POPIA compliance which comes into effect on 01 July 2021.

Fairheads Benefit Services has an appointed and registered Information Officer with the Information Regulator. The Information Officer oversees, monitors and reports on information security compliance with the above Acts including related information security legislation and industry codes. Compliance monitoring and reporting is performed in accordance with the Compliance Risk Management Programme ("CRMP") which is approved by the Assurance, Risk and Compliance Committee. The CRMP is signed off monthly by the Compliance Committee.

Regular testing is performed on our robust IT systems in accordance with a rolling testing schedule managed by the Internal Audit Manager as well as by the external auditor.

A comprehensive compliance risk management assessment has been performed on information security legislation which includes POPIA and PAIA and covers:

- a full analysis of the Act and its regulations
- risk identification
- risk assessment of the information security controls
- risk control register
- risk control gap analysis

A POPIA Impact Analysis has also been undertaken which provides assurance that Fairheads is sufficiently POPIA compliant.

SUMMARY OF POPIA COMPLIANCE MAY 2021

Risk Ratings of Fairheads POPIA readiness	
POPIA Impact Assessment 2021	96.85%
Risk control compliance 2021	95.65%
Annual POPIA Assessment for Staff 2020 (avg %)	92.80%
Statements of Assurance per Dept 2020 (avg%)	100%

Policies and procedures in place to ensure compliance with information security and protection of personal information
Complaints Manual
Confidentiality agreements
Cybersecurity risk cover
Due diligence (3rd parties – service suppliers and providers)
Identification and verification procedures
Information Asset Policy
Information Security and Systems Policy (includes process for investigating and reporting information security incidents)
PAIA Manual (for Company)
PAIA Manual (for funds)
Personal Information Policy (staff)
POPIA compliance statement
Privacy disclaimer (website)
Privacy Policy (Member and Beneficiaries)
Record Management Policy
Record Retention Schedule
Security checks
Third Party Disclosure Procedure

POPIA DUE DILIGENCE

1. ACCOUNTABILITY "The organisation must appoint a party (Information Officer) who will be responsible for ensuring that the information protection principles within POPIA and the controls that are in place to enforce them are complied with."	
Administration Procedures set out the methods for dealing with personal information in compliance with information security legislation.	Y
Agreements between company and service providers/suppliers include confidentiality clauses, information security requirements and compliance.	Y
Annual POPIA assessment for staff	Y
Appointment of Information Officer	Y
Information Security Impact Assessment	Y
Monitoring of POPIA policy implementation	Y
Ongoing POPIA awareness, information and training	Y
PAIA Manual available on website and on request	Y
PAIA Manual for Company	Y
PAIA Manual for funds administered by Fairheads	Y
POPIA Compliance Risk Management Assessment and Framework (POPIA CRMA)	Y
POPIA Gap analysis	Y
POPIA Impact Assessment	Y
POPIA policies have been drafted which set out the rules and guidelines for the collection, processing and storage of personal information and information security requirements.	Y
POPIA risk analysis - risk identification, risk assessment	Y
POPIA risk control register	Y
Staff are suitably trained in the collection, processing and storing of personal information and are bound by a duty of confidentiality not to disclose such information to any person or party, unless authorised to do so or instructed to do so in the public interest or national security.	Y
The company has adequate contracts in place with third party service providers/suppliers and confirms after the performance of due diligence, that these suppliers/providers have appropriate data handling requirements and security safeguards in place.	Y
The company will notify the Fund where it plans to use such service providers to process any Fund information.	Y

2. PROCESS LIMITATION **The second principle deals with the lawfulness of processing, minimality of information collected, consent, justification and objection, and the collection of personal information directly from the data subject**	
Information is collected directly from the data subject and where it is not reasonably practical to collect directly from the data subject, then consent is obtained from the data subject to collect information from a 3rd party.	Y
Information is stored electronically and complies with cloud storage requirements. Hard copy documents are also stored with Metrofile in Cape Town. As per FICA legislation, the FIC is notified of the details of the third-party. Due diligence on the third-party is performed every 3 years in accordance with the Internal Audit schedule. The last due diligence did not identify any non-compliances in terms of Metrofile's POPIA compliance.	Y
The administration business of the company involves the establishment of sub-accounts on behalf of dependants (children/ not lawfully competent) of a deceased member of a retirement fund as per section 37C of the Pension Funds Act. The personal information of children is processed in terms of the Pension Funds Act and is POPIA compliant.	Y
The personal information of children is collected directly from the competent person (guardian/caregiver) in compliance with POPIA's requirements.	Y
3. PURPOSE SPECIFICATION **The third principle provides that personal information must be collected for a specific purpose and the data subject from whom the personal information is collected must be made aware of the purpose for which the personal information was collected.**	
Information is collected directly from the data subject/competent person where it is not reasonably practical to collect directly from the data subject, then consent is obtained from the data subject/ competent person to collect information from a 3rd party.	Y
Personal information in respect of a beneficiary fund or trust is not deleted, destroyed or de-identified. Information is stored electronically and complies with cloud storage requirements. A project is currently underway to limit access to clients' information whose sub-accounts have been terminated. All requests and access to that information will be authorised by the Information Officer. Documents are also stored with Metrofile in Cape Town. As per FICA legislation, the FIC is notified of the details of the third-party. Due diligence on the third-party is performed every 3 years in accordance with the Internal Audit schedule. The last due diligence did not identify any non-compliances in terms of Metrofile's POPIA compliance.	Y
The administration business of the company involves the establishment of sub-accounts on behalf of dependents (children/ not lawfully competent) of a deceased member of a retirement fund as per section 37C of the Pension Funds Act and is lawful. The personal information of children is processed in terms of the Pension Funds Act and is POPIA compliant.	Y
The personal information of children is collected directly from the competent person (guardian/caregiver) and compliance with POPIA's requirements in terms of processing and storage and where it is reasonable, practical and in the best interests of the data subject, from a 3rd party where consent has not been obtained from the competent person (guardian/caregiver).	Y

PRINCIPLE 4: FURTHER PROCESSING LIMITATION **The fourth principle regulates the further processing of personal information. If a responsible party further processes personal information, such processing must be compatible with the purpose for which the information was collected in principle 3.**	
The company will in certain circumstances further process further information on condition that it is in keeping with the initial reason that the information was collected.	Y
PRINCIPLE 5: INFORMATION QUALITY **The responsible party must take reasonable steps to ensure that the personal information that has been collected is complete, accurate, not misleading and up to date. In so doing, the responsible party must take into consideration the purpose for which the personal information was collected.**	
The company, as part of its regular business, performs regular information audits to ensure that clients' information is accurate, not misleading and up to date. Where the information requires correction, the information is updated after identities have been verified.	Y
PRINCIPLE 6: OPENNESS **The responsible party must be open about the collection of personal information by notifying the Regulator if it is going to process personal information and, if personal information is going to be collected, the responsible party must take "reasonably practicable steps to ensure that the data subject has been made aware that his or her personal information is going to be collected. The responsible party should for example, take reasonable steps to make the data subject aware of its name and address, and the purpose for which the personal information is being collected.**	
Communicate new POPI processes with your clients.	Y
Cross border transfer of personal information	Y
Fairheads has suitable privacy notices / statements in its policies and procedures, including the company website which cultivates a culture of openness and transparency regarding information processing activities.	Y
Prior authorisation from the Regulator not applicable (refer to previous comments)	Y
Privacy statement	Y
Purpose Statement	Y
The details of the Regulators including the Information Regulator are made available to all clients at the inception of a sub-account.	Y
There is no restriction on clients to request their own information which is free of charge.	Y
PRINCIPLE 7: SECURITY SAFEGUARDS **The seventh principle provides that the responsible party must ensure that the integrity of the personal information in its control is secured through technical and organisational measures.**	
Access to information is restricted and monitored according to a User Access Register.	Y
Document Management Policy and Record Retention Schedule were updated.	Y
POPIA compliant privacy notice is available on the website.	Y
Records are stored in cloud-based systems but some documents are stored in hardcopy format at Metrofile in Cape Town.	Y
The company has cybersecurity incident cover.	Y
The company has systems in place to continuously monitor and ensure that personal information is held securely at all times.	Y
The Information Security and Systems Policy deals with information security incidents and includes a process for dealing with information security incidents.	Y

PRINCIPLE 8: DATA SUBJECT PARTICIPATION
The eighth principle provides that data subjects have the right to request that a responsible party confirm (free of charge) whether it holds personal information about the data subject, and he or she may also request a description of such information.

Personal information is collected from the Data Subject directly and in cases where information cannot be reasonably or practically be collected from the client, the collection can be justified.

Fairheads, a private body, processes personal information as a Responsible Party. The purpose of the processing is explained clearly to all clients without exception and is set out in the Purpose Statement. The Purpose Statement is sent to each new client at the inception of the sub-account.

PRIOR AUTHORISATION (processing of children's information)

An impact assessment survey was undertaken in March 2021 to establish whether Fairheads Benefit Services requires prior authorisation from the Information Regulator to process information of children. Based on the impact assessment, prior authorisation is not required from the Information Regulator.

In the general and regular administration service, personal information of children is not processed for public consumption. All clients' information is confidential.

Personal information that is collected from competent persons or the data subject is subject to informed consent whereby the data subject/competent person is fully informed of the purpose of the collection and how that information will be used. Personal information is collected to process a request for capital or as supporting documents to a request for capital. The Responsible Party is able to justify the collection of each document that has been collected, processed and stored.

TRANSFER OF INFORMATION CROSS-BORDER

Where personal information is sent cross-border by Fairheads Benefit Services, it is information that requires confirmation in writing from the competent person. That information is sent directly to the data subject/competent person.

Payment information is sent cross-border. Prior to the transfer of this information, the compliance officer ensures that the region has privacy legislation in place or at least privacy standards that comply with South African privacy requirements.

INFORMATION OFFICER

D Van Dieman
compliance@fairheads.com