

PETROSA RETIREMENT FUND

("the Fund")

CONFIDENTIALITY POLICY

1. Purpose

This document constitutes the confidentiality policy for the Board Members and the Principal Officer of the Fund. It is also intended to serve as a policy to be followed by the Fund's service providers.

2. Introduction

2.1. The Board Members, the Principal Officer and the Fund's service providers (here referred to as the "associated Fund parties") are, by virtue of their responsibilities, furnished with and have access to information relating to the Fund's members, employers, investments, and the Fund itself, as well as details pertaining to the operation of the Board of the Fund, all of which is confidential and is "Personal Information" protected under the Protection of Personal Information Act ("POPIA", being Act No. 4 of 2013).

Additionally, POPIA places requirements on the Fund as a Responsible Party (as defined by POPIA) as well as any other Responsible Parties or Operators (as defined by POPIA) linked to the Fund. POPIA applies (with certain allowable exceptions, as outlined in this policy) to the processing of Personal Information (as defined by POPIA) by, or on behalf of, a Responsible Party. The Fund and its Board Members and associated Fund parties must respect the confidentiality of such information in the context of POPIA and other legislative requirements, while demonstrating suitable transparency of operations to retain the trust of the Fund's members and other stakeholders.

As such, it is necessary to set out how these imperatives (transparency and confidentiality within the required legislative context) may be reconciled in a way which reflects good governance.

Board Members and associated Fund parties are expected to comply with the contents of this policy – Board Members and the Principal Officer are required to commit in writing to compliance with the policy.

- 2.2. This policy sets out:-
 - 2.2.1. What information of the Fund is confidential;
 - 2.2.2. The circumstances in which a Board Member or associated Fund party is entitled to have access to confidential information;
 - 2.2.3. The obligation to ensure the protection of the Fund's confidential information; and
 - 2.2.4. Best practices to be adopted with respect to data confidentiality and compliance with POPIA.
- 2.3. This policy must be read in conjunction with the Communication Policy, the Code of Conduct and the POPIA Manual of the Fund.
- 2.4. "Personal information" is very widely defined under POPIA and means information relating to identifiable, living, **natural persons** and identifiable, currently existing, **juristic persons** (legal entities). "Personal information" includes (but is not limited to) such items as gender, race, age, disability, language, "medical, financial, criminal or employment history", and contact details including e-mail address and phone numbers.

3. **Confidential Information**

- 3.1. For the purposes of this policy, "confidential information" excludes information which is in the public domain, or Personal Information which has been de-identified. However, a Board Member or associated Fund party who asserts that information is not confidential because it is in the public domain, bears the onus of demonstrating that such information is in fact in the public domain. In addition, Board members and associated Fund parties should bear in mind that information such as addresses and telephone numbers which are in the public domain are still "Personal Information" as defined in and protected by POPIA.
- 3.2. The confidential information of the Fund, as well as the circumstances in which a Board Member or associated Fund party is entitled to have access to confidential information can be categorised as follows:

Nature of the information	Access to the information
<p>Board information, being</p> <ul style="list-style-type: none"> • minutes of meetings of the Board and any Board sub-committee; • advice received by the Board or any Board sub-committee from the service providers to the Fund (including legal advice whether or not in contemplation of litigation); • any advice provided by a service provider to the Fund in its capacity as such; • any reporting of any nature received by the Board or any Board sub-committee; • any Board appraisal; • any correspondence to or from any Board Member, Principal Officer, or associated Fund party; • any personal information of a Board Member or person who is nominated or proposed as a Board Member; and • any other information relating to the Board, a Board sub-committee or a Board Member which by its nature is confidential or which the Board or a sub-committee categorises as confidential. 	<p>A Board Member or Board sub-committee member has access to all the Board information referred to, including all such relevant Board information prior to that Board Member or Board sub-committee member taking office.</p> <p>This information is not to be disseminated to non-Fund parties in any form unless it is in accordance with a legal requirement and/or has been agreed to by the wider Board and, where applicable, agreed to by the service provider responsible for the information (or to whom the information pertains).</p> <p>For associated Fund parties, including service providers, this information may only be accessed should it be required for the successful completion of actions or services required by the Fund in terms of any contractual agreement and/or falls within the scope of a legislative requirement, and does not infringe on the rights of any other service provider or Fund party.</p> <p>This applies with the exception of any information or details which may be deemed by the Board to be sensitive information and as such should not be disclosed to all or specific Fund parties.</p>

<p>Any information of whatsoever nature relating to, and/or correspondence with, a current or former member, and his or her dependants or beneficiaries, which is in the possession of the Fund, any of its service providers, or any other associated Fund party, whether or not this is in order to carry out services required by the Fund.</p> <p>This specifically includes any data relating to a Fund member.</p>	<p>A Board Member or Board subcommittee member has access to the information pertaining to, and/or correspondence with, a current or former member, and his or her dependants or beneficiaries, only if there is an issue which the Board or subcommittee must decide in relation to that current or former member, or his or her dependants or beneficiaries, such as the quantum of a benefit payable, or how a benefit is to be paid, or in respect of a dispute relating to a benefit or a right to a benefit.</p> <p>A Board Member is not entitled to information relating to a current or former member, or his or her dependants or beneficiaries, merely out of interest, or which does not fall within the specific requirements set out above.</p> <p>Associated Fund parties, including service providers, have access to, hold and/or process the information, and/or correspondence with, a current or former member, and his or her dependants or beneficiaries, only where such information is necessary to successfully perform any duties or actions required by and agreed with the Fund.</p> <p>Although the consent of the individual concerned (or the responsible person in the case of minor children) will not normally be required, any Personal Information relating to such individuals must be collected, held and processed for a specific, explicitly defined and lawful purpose and must not be excessive in</p>
---	---

	<p>relation to the purpose for which it is processed.</p>
<p>Any information relating to an employer which participates, or former employer which previously participated, in the Fund, and which is held by the Fund, or any of its service providers, or any other associated Fund party, whether or not this is in order to carry out services required by the Fund.</p>	<p>A Board Member or any associated Fund party is only entitled to the information and correspondence referred to, to the extent that this is necessary to resolve any issue which has arisen or to perform any required action in respect of the employer.</p>
<p>Any information relating to the operation of the Fund, being:</p> <ul style="list-style-type: none"> • the details of its contractual arrangements; • any litigation or judicial or quasi judicial process in which the Fund is involved; • all correspondence between the Fund, its service providers, any other associated Fund parties, or any other person; • the technical know-how, operational arrangements or proprietary information, whether it has a commercial value or not, of any current or former service provider to the Fund; • the details of any bank accounts operated by the Fund or by any service provider on behalf of the Fund; • the details of any product or investment arrangement in which the Fund is invested; and • the personal details of any current or former Board Member or employee / officer, including the Principal Officer and (where applicable) the Deputy Principal Officer of the Fund, or any service provider to the Fund. 	<p>A Board Member or Board subcommittee member (to the extent that it is relevant to their responsibilities) is entitled to any information relating to the operation of the Fund as set out here.</p> <p>This information is not to be disseminated to non-Fund parties in any form unless it is in accordance with a legal requirement and/or has been agreed to by the Board and, where applicable, agreed to by the service provider responsible for the information (or to whom the information pertains).</p> <p>For all other associated Fund parties, including service providers, this information may only be accessed should it be required for the successful completion of actions or services required by the Fund in terms of any contractual agreement, and/or falls within the scope of a legislative requirement, and does not infringe on the rights of any other service provider or Fund party.</p> <p>This applies with the exception of any information or details which may be deemed by the Board to be sensitive information and as such should not be</p>

	disclosed to all or specific associated Fund parties.
Any other information in the possession of the Fund which the Board or any sub-committee categorises as confidential.	Notwithstanding the provisions above, the Board may at any time determine that any confidential information may not be provided to or accessed by any Board Member or any other associated Fund party; and in that event must provide reasons for that to that Board Member or associated Fund party.

4. Duty to Protect Confidential Information

The Fund and its Board, as a whole, and all associated Fund parties must ensure that the confidential information of the Fund is protected. Accordingly:

- 4.1. Each service provider to the Fund is required to take steps to ensure that the personal information (and any other confidential information) relating to the Fund and its members and their beneficiaries is processed in accordance with the POPIA requirements, and is not accessed unlawfully by any third party, or used for any purpose (whether or not for any financial or other advantage by that service provider or any third party) other than for the purpose for which it is held to provide benefits to the fund membership or to render services to the Fund;
- 4.2. Each Board Member or associated Fund party, including service providers, must not allow any third party to be able to access confidential information of the Fund for the financial advantage, or any other advantage, which the person accessing such information may derive therefrom. For example, a Board Member or administrator may not allow any member data to be accessed by a third party with a view to such third party generating business therefrom.
- 4.3. Personal information (and any other confidential information) relating to the Fund and its members and their beneficiaries, that is held by a service provider, is subject to the retention requirements set out in the POPIA and must, on the termination of the mandate given by the Fund to that service provider, be returned to the Fund, destroyed or retained in the safe custody of that service provider for the benefit of the Fund for such period specified by the Fund (which may be indefinitely so as to protect any legitimate interests, to the extent that this is compatible with the POPIA retention requirements), or any combination of these, in each case as determined by the Board;

- 4.4. Personal information (and any other confidential information) relating to the Fund and its members and their beneficiaries, that is held by a service provider, is subject to the POPIA provisions in respect of trans-border data flows. In the event that the service provider wishes to store such information on servers outside the Republic (e.g. cloud based storage of information), the Fund will require the service provider to ensure that suitable security measures are in place and that the storage of such information accords with both South African data protection laws as well as any foreign laws which may apply.
- 4.5. All Fund information which is held by a Board Member or the Principal Officer, is subject to the retention requirements set out in the POPIA and must, on the Board Member's termination of office be returned to the Fund or destroyed as determined by the Board;
- 4.6. No Board Member or associated Fund party, including service providers, may disclose any confidential information of the Fund to any person who does not have a right to such confidential information. In the event that a Board Member or associated Fund party does (whether intentionally or accidentally) disclose confidential information of the Fund to a person who does not have a right to that confidential information, and this disclosure was not in accordance with an instruction received from the Board or an authorised Fund representative such as the Chairperson of the Fund or the Principal Officer, then that Board Member or associated Fund party must notify the Information Officer of the Fund immediately thereof and also make a disclosure of this to the Board as soon as possible.
- 4.7. No Board Member or associated Fund party, including service providers, may allow confidential information in his / her / their possession to be accessed by any person / entity who has no lawful right to such confidential information. Although a Board Member or associated Fund party may not be able to prevent a person obtaining unlawful access to such confidential information, each Board Member or associated Fund party must take care to ensure that, as far as is reasonably possible, any confidential information in his or her possession is safe-guarded and protected. This extends to measures to ensure the security of such information held on personal communication devices such as smartphones, tablets and laptop computers, as well as information held in documentary (paper) form. Best practices are outlined in section 5.
- 4.8. The Board must ensure that the confidential information of the Fund is stored in a way that will be accessible in the future, unless the Board is reasonably certain that the retention of such confidential information does not, and never will, serve any practical purpose.

5. Best practices in accordance with data confidentiality and the POPIA

- 5.1. The following best practices should be adhered to by the Fund, its Board Members, and any other associated Fund party, including service providers:

- 5.1.1. Password protection should be applied to all electronically distributed Fund documents, particularly when such documentation may contain sensitive or member related information. Passwords should be changed regularly and should be communicated separately (e.g. by Whatsapp or SMS or in a separate email), i.e. passwords should not be sent with the documents themselves.
- 5.1.2. Where practically possible, member information should be suitably “de-identified” in Fund documentation, unless the identifying information is necessary in the context of a required decision, is required to comply with a legal obligation, or is needed to protect the legitimate interest of a data subject.
- 5.1.3. “Hard” copies (i.e. printed copies) of any Fund documentation must be limited to the extent possible, since these may be easily intercepted or misplaced. If hard copies containing members’ personal information are distributed in a meeting, best practice would normally be to collect and destroy these at the end of the meeting. The Fund should avoid the practice of circulating hard copies of documents such as “agenda packs”, where these include members’ personal information, in advance of meetings – best practice is to circulate such documents in password-protected electronic form.
- If such hard copies are provided, these should be safeguarded and kept in a safe place and not lying around where unauthorised persons may have sight of it or be able to access it.
- 5.1.4. In the usual course of events, only company email addresses and other electronic devices may be used for the processing of any and all Fund information (the assumption here is that the relevant companies will have adequate security protections in place). All Fund parties must take personal responsibility for the encryption of all devices on which any information pertaining to the Fund is stored or processed and the security of passwords and email accounts, noting that a “data breach” must be reported to the Board and then to the Information Regulator as well as the affected members, as noted in paragraph 6.
- 5.1.5. All Fund parties must secure the integrity and confidentiality of Personal Information in their possession or under their control by taking appropriate technical and organisational measures to prevent loss or unlawful access of such information, and must also employ regularly updated safeguards against any internal or external risks.

As such, all Fund parties must review the suitability of security levels on electronic devices used for Fund and related information, and security levels applying to e-mail accounts and electronic data storage, so as to ensure compliance with this

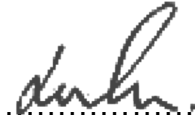
policy. Board Members are required to accept personal responsibility in this regard.

5.1.6. All Fund parties are not to allow any external non-Fund parties (e.g. family members, colleagues, friends) to access devices with Fund information, or if they do they must ensure that the Fund information is not accessible to the said parties on those devices.

5.1.7. Contribution schedules sent by the participating employer(s) and all other personal information relating to Fund members are to be disseminated only to those parties who are authorised to view such information. The service provider(s) handling this information must ensure that suitable safeguards have been set in place (e.g. password protected documents).

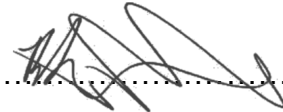
6. All Fund parties are to respect and abide by the contents of this policy and, where necessary, communicate any known data / security breaches to the Information Officer as soon as possible, regardless of whether such breach was caused by him / her / itself or by any other Fund party.

Adopted by the Board on **26 September 2023**



.....

Chairperson



.....

Principal Officer