INTERNAL POPIA POLICY

Title:	OPFA: Internal POPIA Policy
Custodian:	Information Officer/Deputy Information Officer
Prepared By:	Senior Legal Advisor
Date Created:	February 2021
Version No:	V2
Reference No.	TBA
Date Approved:	18/03/2024
Effective Date:	Date of Accounting Authority Approval
Approved By:	Accounting Authority

Document owner:

NAME	POSITION
Nondumiso Ntshangase	Deputy Information Officer

Mandatory Review period:

To be reviewed every second year or when significant changes occur

Version Control Page

This page should provide a history of previous versions of the policy and changes made:

Version	Date	Author	Status	Comment / changes
1	01/02/2021	OPFA ManCo	Approved	First version
2	18/03/2024	OPFA ManCo	Reviewed and approved	Minor changes

TABLE OF CONTENTS

OPFA
Internal POPIA Policy

1. PREAMBLE

The right to privacy is an integral human right recognised and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 ("POPIA").

POPIA aims to promote the protection of privacy by providing guiding principles that are intended to be applied to the processing of Personal Information in a context-sensitive manner.

The OPFA is a public body as determined in POPIA and is allowed to process personal information while exercising and performing its powers, duties, and functions in terms of the requirements set in the Pension Funds Act, Nr 24 of 1956 ("PFA"), in accordance with POPIA and the PFA regulations regarding the processing of personal information. This applies to the OPFA's functions in relation to disposing of a complaint i.e., it does not relate to other business functions such as corporate support and human resources.

Through the provision of Ombud services, the OPFA is necessarily involved in the collection, use and disclosure of certain aspects of the Personal Information of parties to a complaint, employees, service providers and other stakeholders.

A person's right to privacy entails having control over his or her Personal Information and being able to conduct his or her affairs relatively free from unwanted intrusions.

POPIA does not apply to the judicial functions performed by the OPFA. In exercising its powers, duties, and functions under the PFA, in the course of disposing of complaints in terms of Chapter VA of the Pension Funds Act, 1956, the OPFA fully embraces the principles and objectives of POPIA when disposing of complaints, insofar as it may be reasonably practical to do so. Given the importance of privacy, the OPFA is committed to effectively managing Personal Information in accordance with the provisions of POPIA.

2. DEFINITIONS

"Personal Information" is any information that can be used to reveal a person's identity. Personal Information relates to an identifiable, living, natural person, and where applicable,

an identifiable, existing juristic person (such as a company), including, but not limited to information concerning—

- race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language, and birth of a person;
- 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 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;
- 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.

"Data Subject" refers to the natural or juristic person to whom Personal Information relates, such as an individual employee or a service provider that supplies the OPFA with products or services or other stakeholder but shall not include parties to a complaint as defined below.

"Responsible Party" is the entity that needs the Personal Information for a particular reason and determines the purpose of and means for processing the Personal Information. In this case, the OPFA is the Responsible Party.

"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. For example, a third-party service provider that has contracted with the OPFA to shred documents containing Personal Information.

"Information Officer" means the person responsible for ensuring the OPFA's compliance with POPIA.

- Where no Information Officer is appointed, the head of the OPFA will be responsible for performing the Information Officer's duties.

- Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.

"parties to a complaint" means those persons referred to in section 30G of the Pension Funds Act, 1956.

"Processing" means the act of processing information and includes any activity or any set of operations, whether or not 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;
- merging, linking, as well as any restriction, degradation, erasure, or destruction of information.

"Record" 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;
- 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;
- Photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced.

"Filing System" means any structured set of Personal Information, whether centralised, decentralised, or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

"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.

"De-Identify" means to delete any information that identifies a Data Subject, or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the Data Subject.

"Re-Identify", means, in relation to the Personal Information of a Data Subject, to resurrect any information that has been de-identified that identifies the Data Subject, or can be used or manipulated by a reasonably foreseeable method to identify the Data Subject.

"Consent" means any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of Personal Information.

"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.

3. POLICY PURPOSE

The purpose of this policy is to protect the OPFA from the compliance risks associated with the protection of Personal Information which includes:

- Breaches of confidentiality. For instance, the OPFA could suffer litigation losses where it is found that the Personal Information of Data Subjects has been shared or disclosed unlawfully;
- Failing to offer choice. For instance, all Data Subjects should be free to choose how and for what purpose the OPFA uses information relating to them;
- Reputational damage. For instance, the OPFA could suffer a decline in stakeholder trust following an adverse event such as a computer hacker deleting the Personal Information held by the OPFA;
- This policy demonstrates the OPFA's commitment to protecting the privacy rights of Data Subjects in the following manner:
  - Through stating desired behaviour and directing compliance with the provisions of POPIA and best practice;
  - By cultivating an organisational culture that recognises privacy as a valuable human right;
  - By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of Personal Information;

- By creating business practices that will provide reasonable assurance that the rights of Data Subjects are protected and balanced with the legitimate business needs of the OPFA.
- By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information Officers, in order to protect the interests of the OPFA and Data Subjects.
- By raising awareness through training and providing guidance to individuals who process Personal Information so that they can act confidently and consistently.

4. POLICY APPLICATION

This policy and its guiding principles apply to:

- The OPFA;
- All business units and divisions of the OPFA;
- All employees and volunteers; and
- All contractors, suppliers and any other persons acting on behalf of the OPFA.

The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as the OPFA's PAIA Manual as required by the Promotion of Access to Information Act (Act No 2 of 2000).

The legal duty to comply with POPIA's provisions is activated in any situation where there is a processing of Personal Information and entered into any record by or for the OPFA.

POPIA does not apply in situations where the processing of Personal Information—

- is concluded in the course of purely personal or household activities,
- where the Personal Information has been de-identified,
- by or on behalf of a public body—

  (i) which involves national security, including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, defence, or public safety; or

  (ii) the purpose of which is the prevention, detection, including assistance in the identification of the proceeds of unlawful activities and the combating of money laundering activities, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures,

  to the extent that adequate safeguards have been established in legislation for the protection of such personal information;

- by the Cabinet and its committees or the Executive Council of a province; or
- relating to the judicial functions of a court referred to in section 166 of the Constitution.

POPIA does not apply to the judicial functions performed by the OPFA in the course of disposing of complaints in terms of Chapter VA of the Pension Funds Act, 1956. Notwithstanding, and insofar as it may be reasonably practical to do so, the OPFA fully embraces the principles and objectives of POPIA when disposing of complaints. The measures implemented by the OPFA to do so are set out in the OPFA policies pertaining to Personal Information, including this policy.

5. RIGHTS OF DATA SUBJECTS

Where appropriate, the OPFA will ensure that Data Subjects are made aware of the rights conferred upon them.

The OPFA will ensure that it gives effect to the following six rights.

5.1. THE RIGHT TO ACCESS PERSONAL INFORMATION

The OPFA recognises that a Data Subject has the right to establish whether the OPFA holds Personal Information related to him, her, or it, including the right to request access to that Personal Information.

In terms of this policy, the right to access personal information shall also apply to parties to a complaint.

5.2. THE RIGHT TO HAVE PERSONAL INFORMATION CORRECTED OR DELETED

The Data Subject has the right to request, where necessary, that his, her or its Personal Information must be corrected or deleted where the OPFA is no longer authorised to retain the Personal Information.

In terms of this policy, the right to have personal information corrected or deleted shall apply to parties to a complaint during the course of an investigation but shall not apply once a determination is issued. Once a determination has been issued by the OPFA, the OPFA is legally obliged in terms of section 30L of the Pension Funds Act, 1956 to maintain a permanent record of the proceedings relating to the adjudication of a complaint and the evidence given. Should a party to a complaint request that their personal information is corrected after the

issuing of a determination, such new personal information provided shall be separately attached to the record however the previous personal information provided will not be deleted.

5.3. THE RIGHT TO OBJECT TO THE PROCESSING OF PERSONAL INFORMATION

The Data Subject has the right, on reasonable grounds, to object to the processing of his, her or its Personal Information. In such circumstances, the OPFA will give due consideration to the request and the requirements of POPIA. The OPFA 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 the Personal Information.

In terms of this policy, the parties to a complaint will be informed that any personal information provided to the OPFA will be processed for the purpose of disposing of the complaint in terms of Chapter VA of the Pension Funds Act, 1956. Parties to a complaint shall be further informed that by providing personal information to the OPFA, the parties to the complaint tacitly consent to the processing of such personal information.

5.4. THE RIGHT TO COMPLAIN TO THE INFORMATION REGULATOR

The Data Subject and parties to a complaint have the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its Personal Information.

5.5. THE RIGHT TO BE INFORMED

The Data Subject has the right to be notified that his, her or its Personal Information is being collected by the OPFA. The Data Subject and parties to a complaint have the right to be notified in any situation where the organisation has reasonable grounds to believe that the Personal Information of the Data Subject or party to a complaint has been accessed or acquired by an unauthorised person.

6. GENERAL GUIDING PRINCIPLES

All employees and persons acting on behalf of the OPFA will at all times be subject to, and act in accordance with, the following guiding principles:

6.1. ACCOUNTABILITY

Failing to comply with POPIA could potentially damage the OPFA's reputation or expose the OPFA to a civil claim for damages. The protection of Personal Information is therefore everybody's responsibility.

The OPFA will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, the OPFA will take appropriate sanctions, which may include disciplinary action, against those individuals who, through their intentional or negligent actions and/or omissions, fail to comply with the principles and responsibilities outlined in this policy.

6.2. PROCESSING LIMITATION

The OPFA will ensure that Personal Information under its control is processed:

- in a fair, lawful, and non-excessive manner, and
- only with the informed consent of the Data Subject, and
- only for a specifically defined purpose.

The OPFA will inform the Data Subject of the reasons for collecting his, her or its Personal Information and obtain written consent prior to processing Personal Information. Alternatively, where services or transactions are concluded over the telephone or electronic video feed, the OPFA will, where possible, maintain a voice recording of the stated purpose for collecting the Personal Information followed by the Data Subject's subsequent consent.

The OPFA will under no circumstances distribute or share Personal Information between separate legal entities, associated organisations (such as subsidiary companies) or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected.

Where applicable, the Data Subject must be informed of the possibility that their Personal Information will be shared with other areas of the OPFA's business and be provided with the reasons for doing so.

6.3. PURPOSE SPECIFICATION

All the OPFA's business units and operations must be informed of the principle of transparency.

The OPFA will process Personal Information only for specific, explicitly defined, and legitimate reasons. The OPFA will inform Data Subjects of these reasons prior to collecting or recording the Data Subject's Personal Information.

6.4. FURTHER PROCESSING LIMITATION

Personal Information will not be processed for a secondary purpose unless that processing is compatible with the original purpose.

Therefore, where the OPFA seeks to process Personal Information, it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, the OPFA will first obtain additional consent from the Data Subject.

6.5. INFORMATION QUALITY

The OPFA will take reasonable steps to ensure that all Personal Information collected is complete, accurate and not misleading.

The more important it is for the Personal Information to be accurate (for example, the beneficiary details of a life insurance policy are of the utmost importance), the greater the effort the OPFA will put into ensuring its accuracy.

Where Personal Information is collected or received from third parties, the OPFA will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the Data Subject or by way of independent sources.

6.6. OPEN COMMUNICATION

The OPFA will take reasonable steps to ensure that Data Subjects are notified (are at all times aware) that their Personal Information is being collected including the purpose for which it is being collected and processed.

The OPFA will ensure that it establishes and maintains a “contact us” facility, for instance via its website or through an electronic helpdesk, for Data Subjects who want to—

- enquire whether the OPFA holds related Personal Information, or
- request access to related Personal Information, or
- request the OPFA to update or correct related Personal Information, or
- make a complaint concerning the processing of Personal Information.

6.7. SECURITY SAFEGUARDS

The OPFA will manage the security of its filing / data record-keeping system to ensure that Personal Information is adequately protected. To this end, security controls will be implemented to minimise the risk of loss, unauthorised access, disclosure, interference, modification, or destruction.

Security measures also need to be applied in a context-sensitive manner. For example, the more sensitive the Personal Information, such as medical information or credit card details, the greater the security required.

The OPFA will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on the OPFA's IT network. The OPFA will ensure that all paper and electronic records comprising Personal Information are securely stored and made accessible only to authorised individuals.

All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of Personal Information for which the OPFA is responsible.

All existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment containing the relevant consent and confidentiality clauses.

The OPFA's operators and third-party service providers will be required to enter into service level agreements with the organisation where both parties pledge their mutual commitment to POPIA and the lawful processing of any Personal Information pursuant to the agreement.

The failure to sign an employment contract, addendum, or service level agreement, as referred to above, does not absolve any employee, operator, or third-party service provider from their obligations to comply with legislative requirements pertaining to the protection of Personal Information and the provisions of this policy.

6.8. DATA SUBJECT PARTICIPATION

A Data Subject may request the correction or deletion of his, her or its Personal Information held by the OPFA.

The OPFA will ensure that it provides a facility for Data Subjects who want to request the correction or deletion of their Personal Information.

Where applicable, the OPFA will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

7. INFORMATION OFFICERS

The OPFA will appoint an Information Officer and where necessary, a Deputy Information Officer to assist the Information Officer.

The OPFA's Information Officer is responsible for ensuring compliance with POPIA.

Where no Information Officer is appointed, the head of the OPFA will assume the role of the Information Officer.

Consideration will be given on an annual basis to the re-appointment or replacement of the Information Officer and the re-appointment or replacement of any Deputy Information Officers.

Once appointed, the OPFA will register the Information Officer, and the Deputy Information Officer, where applicable, with the South African Information Regulator established under POPIA prior to performing his or her duties.

8. SPECIFIC DUTIES AND RESPONSIBILITIES

8.1. OPFA AS GOVERNING BODY

The OPFA cannot delegate its accountability and is ultimately answerable for ensuring that the OPFA meets its legal obligations in terms of POPIA.

The OPFA may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

The OPFA is responsible for ensuring that:

- The OPFA appoints an Information Officer, and where necessary, a Deputy Information Officer;
- All persons responsible for the processing of Personal Information on behalf of the OPFA—
  - are appropriately trained and supervised to do so;
  - understand that they are contractually obligated to protect the Personal Information they come into contact with, and

  - are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.
- Data Subjects who want to make enquiries about their Personal Information are made aware of the procedure that needs to be followed should they wish to do so;
- Periodic POPIA Audits are scheduled in order to accurately assess and review the ways in which the OPFA collects, holds, uses, shares, discloses, destroys, and processes Personal Information.

8.2. INFORMATION OFFICER

The OPFA's Information Officer is responsible for:

- Taking steps to ensure the OPFA's reasonable compliance with the provision of POPIA;
- Keeping the OPFA updated about the OPFA's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of its obligations pursuant to POPIA;
- Continually analysing privacy legislation and aligning them with the OPFA's Personal Information processing procedures. This will include reviewing the OPFA's information protection procedures and related policies;
- Ensuring that POPIA Audits are scheduled and conducted on a regular basis;
- Ensuring that the OPFA makes it convenient for Data Subjects who want to update their Personal Information or submit POPIA related complaints to the OPFA. For instance, maintaining a "contact us" facility on the OPFA's website;
- Approving any contracts entered into with Operators, employees and other third parties which may have an impact on the Personal Information held by the OPFA. This will include overseeing the amendment of the OPFA's employment contracts and other service level agreements.
- Encouraging compliance with the conditions required for the lawful processing of Personal Information;
- Ensuring that employees and other persons acting on behalf of the OPFA are fully aware of the risks associated with the processing of Personal Information, and that they remain informed about the OPFA's security controls;
- Organising and overseeing the awareness training of employees and other individuals involved in the processing of Personal Information on behalf of the OPFA;
- Addressing employees' POPIA related questions;
- Addressing all POPIA related requests/complaints made by the OPFA's Data Subjects;

- Working with the Information Regulator in relation to any ongoing investigations. The Information Officer and Deputy Information Officer will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of Personal Information and will consult with the Information Regulator where appropriate, with regard to any other matter. The Deputy Information Officer will assist the Information Officer in performing his or her duties.

8.3. IT MANAGER

The OPFA's IT Manager is responsible for:

- Ensuring that the OPFA's IT infrastructure, filing systems and any other devices used for processing Personal Information meet acceptable security standards;
- Ensuring that all electronically held Personal Information is kept only on designated drives and servers and uploaded only to approved cloud computing services;
- Ensuring that servers containing Personal Information are sited in a secure location, away from the general office space;
- Ensuring that all electronically stored Personal Information is backed-up and tested on a regular basis;
- Ensuring that all back-ups containing Personal Information are protected from unauthorised access, accidental deletion, and malicious shacking attempts;
- Ensuring that Personal Information being transferred electronically is encrypted;
- Ensuring that all servers and computers containing Personal Information are protected by a firewall and the latest security software;
- Performing regular IT audits to ensure that the security of the OPFA's hardware and software systems are functioning properly;
- Performing regular IT audits to verify whether electronically stored Personal Information has been accessed or acquired by any unauthorised persons;
- Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process Personal Information on the OPFA's behalf. For instance, on cloud computing services.

8.4. COMMUNICATION

The OPFA's Information Office is responsible for:

- Approving and maintaining the protection of Personal Information statements and disclaimers that are displayed on the OPFA's website, including those attached to communications such as emails and electronic newsletters;

- Addressing any Personal Information protection queries from journalists or media outlets such as newspapers;
- Where necessary, working with persons acting on behalf of the OPFA to ensure that any outsourced communication initiatives comply with POPIA.

8.5. EMPLOYEES AND OTHER PERSONS ACTING ON BEHALF OF THE OPFA

Employees and other persons acting on behalf of the OPFA will, during the course of the performance of their services, gain access to and become acquainted with the Personal Information of certain clients, suppliers, and other employees.

Employees and other persons acting on behalf of the OPFA are required to treat Personal Information as a confidential business asset and to respect the privacy of Data Subjects.

Employees and other persons acting on behalf of the OPFA may not directly or indirectly, utilise, disclose, or make public in any manner to any person or third party, either within the OPFA or externally, any Personal Information, unless such information is already publicly known, or the disclosure is necessary in order for the employee or person to perform his or her duties.

Employees and other persons acting on behalf of the OPFA must request assistance from their line manager or the Information Officer if they are unsure about any aspect related to the protection of a Data Subject's Personal Information.

Employees and other persons acting on behalf of the OPFA will only process Personal Information where:

- The Data Subject, or a competent person where the Data Subject is a child, consents to the processing; or
- The processing is necessary to carry out actions for the conclusion or performance of a contract to which the Data Subject is a party; or
- The processing complies with an obligation imposed by law on the OPFA as Responsible Party; or
- The processing protects a legitimate interest of the Data Subject; or
- The processing is necessary for pursuing the legitimate interests of the OPFA or of a third party to whom the information is supplied; or
- The processing is necessary for the disposal of complaints as contemplated in Chapter VA of the Pension Funds Act, 1956.

Furthermore, Personal Information will only be processed where the Data Subject:

- Clearly understands why and for what purpose his, her or its Personal Information is being collected; and
- Has granted the OPFA with explicit written or verbally recorded consent to process his, her or its Personal Information.

Employees and other persons acting on behalf of the OPFA will consequently, prior to processing any Personal Information, obtain from the Data Subject permission for the processing of Personal Information.

Informed consent is therefore when the Data Subject clearly understands for what purpose his, her or its Personal Information is needed and who it will be shared with.

Consent from a Data Subject can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, the OPFA will keep, where possible, a voice recording of the Data Subject's consent in instances where transactions are concluded telephonically or via electronic video feed.

Consent to process a Data Subject's Personal Information will be obtained directly from the Data Subject, except where—

- the Personal Information has been made public; or
- where valid consent has been given to a third party; or
- the information is necessary for effective law enforcement; or
- the processing is necessary for the disposal of complaints as contemplated in Chapter VA of the Pension Funds Act, 1956.

Employees and other persons acting on behalf of the OPFA will under no circumstances:

- Process or have access to Personal Information where such processing or access is not a requirement to perform their respective work-related tasks or duties;
- Save copies of Personal Information directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All Personal Information must be accessed and updated from the OPFA's central database or a dedicated server;
- Share Personal Information informally.
- Transfer Personal Information outside of South Africa without the express permission from the Information Officer. Employees and other persons acting on behalf of the OPFA are responsible for—
  - keeping all Personal Information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy;

- ensuring that Personal Information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created;
- ensuring that Personal Information is encrypted prior to sending or sharing the information electronically. The IT Manager will assist employees and where required, other persons acting on behalf of the OPFA, with the sending or sharing of Personal Information to or with authorised external persons;
- ensuring that all computers, laptops, and devices such as tablets, flash drives and smartphones that store Personal Information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons;
- ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks;
- ensuring that where Personal Information is stored on removable storage medias e.g. external drives/CDs/DVDs that these are kept locked away securely when not in use;
- ensuring that where Personal Information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer of a filing cabinet;
- ensuring that where Personal Information has been printed, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer;
- taking reasonable steps to ensure that Personal Information is kept accurate and up to date. For instance, confirming a Data Subject's contact details when the client or customer phones or communicates via email. Where a Data Subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the Information Officer to update the information accordingly;
- taking reasonable steps to ensure that Personal Information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where Personal Information is no longer required, authorisation must first be obtained from the relevant line manager or the Information Officer to delete or dispose of the Personal Information in the appropriate manner;
- undergoing POPIA Awareness training from time to time.

Where an employee, or a person acting on behalf of the OPFA, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction, or the unsanctioned disclosure of Personal Information, he or she must

immediately report this event or suspicion to the Information Officer or the Deputy Information Officer.

9. POPIA AUDIT

The OPFA's Information Officer will schedule periodic POPIA Audits.

The purpose of a POPIA audit is to:

- Identify the processes used to collect, record, store, disseminate and destroy Personal Information;
- Determine the flow of Personal Information throughout the OPFA. For instance, the OPFA's various business units, divisions, branches, and other associated organisations;
- Redefine the purpose for gathering and processing Personal Information;
- Ensure that the processing parameters are still adequately limited;
- Ensure that new Data Subjects are made aware of the processing of their Personal Information;
- Re-establish the rationale for any further processing where information is received via a third party;
- Verify the quality and security of Personal Information;
- Monitor the extent of compliance with POPIA and this policy;
- Monitor the effectiveness of internal controls established to manage the OPFA's POPIA related compliance risk.

In performing the POPIA Audit, the Information Officer and Deputy Information Officer will liaise with line managers in order to identify areas within in the OPFA's operation that are most vulnerable or susceptible to the unlawful processing of Personal Information.

The Information Officer and Deputy Information Officer will be permitted direct access to and have demonstrable support from line managers and the OPFA's governing body in performing their duties.

10. REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

Data Subjects and parties to a complaint have the right to:

- Request what Personal Information the OPFA holds about them and why;
- Request access to their Personal Information, and

- Be informed how to keep their Personal Information up to date.

Access to information requests can be made by email, addressed to the Information Officer. The Information Officer will provide the Data Subject or party to a complaint with a “Personal Information Request Form”.

Once the completed form has been received, the Information Officer will verify the identity of the Data Subject or party to a complaint prior to handing over any Personal Information. All requests will be processed and considered against the OPFA’s PAIA Policy.

The Information Office will process all requests within a reasonable time.

11. POPIA COMPLAINTS PROCEDURE

Data Subjects and parties to a complaint have the right to complain in instances where they believe that any of their rights under POPIA have been infringed upon. The OPFA takes all complaints very seriously and will address all POPIA related complaints in accordance with the following procedure:

- POPIA complaints must be submitted to the OPFA in writing. Where so required, the Information Officer will provide the Data Subject or parties to a complaint with a “POPIA Complaint Form”.
- Where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within 1 working day;
- The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days;
- The Information Officer will carefully consider the complaint and address the complainant’s concerns in an amicable manner. In considering the complaint, the Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA;
- The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on the OPFA’s Data Subjects or parties to a complaint;
- Where the Information Officer has reason to believe that the Personal Information of Data Subjects or parties to a complaint has been accessed or acquired by an unauthorised person, the Information Officer will consult with the OPFA’s governing

body where after the affected Data Subjects or parties to a complaint and the Information Regulator will be informed of this breach;

- The Information Officer will revert to the POPIA complainant with a proposed solution with the option of escalating the complaint to the OPFA's governing body within 7 working days of receipt of the complaint or such period as may be reasonable in the circumstances. In all instances, the OPFA will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines;
- The Information Officer's response to the Data Subject may comprise any of the following:
  - A suggested remedy for the complaint;
  - A dismissal of the complaint and the reasons as to why it was dismissed;
  - An apology (if applicable) and any disciplinary action that has been taken against any employees involved.
- Where the Data Subject or party to a complaint is not satisfied with the Information Officer's suggested remedies, the Data Subject or party to a complaint has the right to complain to the Information Regulator;
- The Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPIA related complaints.

12. DISCIPLINARY ACTION

Where a POPIA complaint or a POPIA infringement investigation has been finalised, the OPFA may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy.

In the case of ignorance or minor negligence, the OPFA will undertake to provide further awareness training to the employee.

Any gross negligence or the wilful mismanagement of Personal Information, will be considered a serious form of misconduct for which the OPFA may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.

Examples of immediate actions that may be taken subsequent to an investigation include:

- A recommendation to commence with disciplinary action;
- A referral to appropriate law enforcement agencies for criminal investigation;
- Recovery of funds and assets in order to limit any prejudice or damages caused.

ANNEXURE

Declaration and Consent

I, _____,
acknowledge that I have read and understand the contents of the OPFA‘s Internal POPIA Policy.

I agree to:

a) Honour my duties and responsibilities in terms of POPIA at all times;
b) Adhere to the OPFA‘s POPIA Policy at all times, and apply the guidelines contained herein to my daily tasks and responsibilities;
c) Direct all POPIA related enquiries to the OPFA’s Information Officer, where I am uncertain about the requirements and/or application thereof.

Signed at _____ on _____

_____

(Signature)