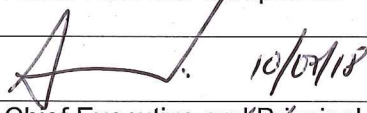











## Eskom Pension and Provident Fund ("EPPF")

### Privacy Policy

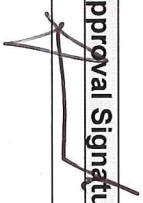
Policy Reference Number	[Policy number]
Version Number	Version 1.0
Effective Date	6 June 2018
Review Date	June 2021
Policy Owner	Head: Risk and Compliance
Signature	 10/07/18
Policy Sponsor	Chief Executive and Principal Officer
Signature	
Date Approved	11/07/2018

# Key Stakeholders in implementing and monitoring this Policy




Stakeholder	Designation	Approval Signature	Date
Executive Management	Chief Executive/Principal Officer		11/07/2018
Investment Management Unit	Chief Investment Officer		10/7/2018
Finance	Chief Financial Officer (Acting)		10/7/2018
Retirement Fund Operations	Head: Retirement Fund Operations		10/7/2018
Risk and Compliance Management	Head: Risk and Compliance		10/9/2018
Legal and Corporate Secretariat	Head: Legal and Corporate Secretariat		10/7/2018
Information Technology	Head: Information Technology		10/7/2018
Human Resources	Head: Human Resources		10/07/2018

### Recommended by Policy Owner

I hereby acknowledge that we have reviewed this policy is not duplicated or in conflict with any other policies.

Role	Designation	Approval Signature	Date
Policy Owner	Head: Risk and Compliance		10/07/18

### Final Approval

Role	Designation	Approval Signature	Date
Policy Sponsor	Chief Executive/Principal Officer		11/07/2018
Legal and Governance Committee	Chairman of Legal and Governance Committee		27/07/2018
Board of Fund	Chairman of the Board of Fund		27/07/2018

### Summary of Version Control

Version Number	Effective Date	Reason for Change	Summary of Changes
Version 1.0			

## Table of Contents

1. INTRODUCTION.....	6
2. PURPOSE.....	6
3. DEFINITION.....	6
4. SCOPE .....	8
5. POLICY STATEMENT .....	8
6. ROLES AND RESPONSIBILITIES .....	12
7. RELATED INFORMATION AND REFERENCE.....	14
8. EXCLUSIONS .....	14
9. REQUEST TO DEVIATE FROM POLICY .....	14
10. COMPLIANCE MONITORING.....	14
11. NON-COMPLAINE.....	15

## 1. INTRODUCTION

- 1.1. The Protection of Personal Information Act 4 of 2013 (POPIA) gives effect to the constitutional right to privacy in terms of Section 14 of the Bill of Rights of the Constitution of South Africa. Non-compliance with the POPIA can result in penalties and damage to the Fund's reputation.

## 2. PURPOSE

The objectives of this Policy are to:

- 2.1. Establish accountability for the lawful Processing of the Personal Information of the Fund's Data Subjects.
- 2.2. Ensure the Fund and its operators adequately and lawfully process Personal Information of its Data Subjects.
- 2.3. Provide for the adequate protection of Personal Information processed by the Fund or its operators, irrespective of format.
- 2.4. Educate Users of Personal Information on the rights of Data Subjects to access their Personal Information held by the Fund or its Operators who are Processing Personal Information on behalf of the Fund.

## 3. DEFINITION

- 3.1. The following definitions are relevant to this Privacy Policy.

Term	Definition
<b>Board</b>	The Board of Trustees of the Fund.
<b>Data Subject</b>	The natural or juristic person to whom the Personal Information relates.
<b>Effective date</b>	The date on which this Policy shall become of force and effect.
<b>EPPF/ Fund</b>	The Eskom Pension and Provident Fund
<b>Employee</b>	An employee of the Fund and for the purposes of this Policy will include contractors, service providers and temporary staff who have been granted access to and approval to use the EPPF's information resources.
<b>EXCO / Management</b>	The Executive Management Committee of the Fund
<b>Line Manager</b>	An Employee who by virtue of his position and seniority has been granted the authority to manage the work activities of another Employee or group of Employees.
<b>PAIA</b>	Promotion of Access to Information Act 2 of 2000
<b>Operator</b>	A natural or juristic person who processes Personal Information for a responsible party (in terms of this Policy, the Fund) in terms of a contract or mandate, without coming under the direct authority of the responsible party.
<b>Personal Information</b>	Personal Information is defined as information relating to an identifiable, living, natural person and where applicable, an identifiable, existing juristic person including, but not limited to –



Term	Definition
	<ul style="list-style-type: none"> <li>• 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, conscious, belief, culture, language and birth of the person;</li> <li>• information relating to the education or the medical, financial, criminal or employment history of the person;</li> <li>• any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;</li> <li>• the biometric information of the person;</li> <li>• the personal opinions, views or preferences of the person;</li> <li>• 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;</li> <li>• the views or opinions of another individual about the person; and</li> <li>• 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.</li> </ul>
<b>Policy</b>	The Privacy Policy
<b>Policy Owner</b>	The designated position in the organisation that can modify the Policy, drive compliance to the Policy and is responsible for the inclusion of future updates / changes to the Policy.
<b>POPIA</b>	Protection of Personal Information Act 4 of 2013
<b>Processing</b>	<p>Any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information (refer to the POPIA Act) which includes:</p> <ul style="list-style-type: none"> <li>• collection, receipt, recording, organising, collating, storing, updating, modifying, retrieving, altering, distributing by transmission, distribution or making available in any form, merging, linking, restricting degrading, erasing and/or destroying.</li> </ul>
<b>Record</b>	<p>Any recorded information—</p> <ul style="list-style-type: none"> <li>• regardless of form or medium, including any of the following: <ul style="list-style-type: none"> <li>○ Writing on any material;</li> <li>○ 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;</li> <li>○ label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;</li> <li>○ book, map, plan, graph or drawing;</li> <li>○ 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;</li> </ul> </li> <li>• in the possession or under the control of a responsible party;</li> </ul>

Term	Definition
	<ul style="list-style-type: none"> <li>• whether or not it was created by a responsible party; and</li> <li>• regardless of when it came into existence.</li> </ul>
<b>Responsible Party</b>	<p>A public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for, Processing Personal Information.</p> <p>The Fund is the Responsible Party regarding the Personal Information processed by the Fund, or processed on behalf of the Fund by its Operators.</p>
<b>Review Date</b>	The date on which this Policy should be reviewed again for any updates and changes.
<b>Special Personal Information</b>	<p>Special Personal Information includes the following:</p> <ul style="list-style-type: none"> <li>• 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; or</li> <li>• the criminal behaviour of a Data Subject to the extent that such information relates to— <ul style="list-style-type: none"> <li>• the alleged commission by a Data Subject of any offence; or</li> <li>• any proceedings in respect of any offence allegedly committed by a Data Subject or the disposal of such proceedings.</li> </ul> </li> </ul>
<b>User</b>	Includes all Fund employees and third parties who make use of and have access to Fund systems used for the Processing of Personal Information.

## 4. SCOPE

4.1. This Policy limits the discretion of the trustees, the officers and the other employees of the Fund, all contractors of the Fund, all suppliers and outsource service providers (“operators”), and any other person or organisation authorised to process Personal Information on behalf of the Fund.

4.2. All forms of Processing of Personal Information in any format are subject to this Policy.

## 5. POLICY STATEMENT

### 5.1. Accountability

The Fund will ensure that all Processing conditions are complied with at the time of Processing of all Personal Information. In pursuance of compliance with these, the Fund will adhere to the following:

5.1.1. A privacy governance structure will be defined and formal privacy reporting established;

5.1.2. A formal Privacy Policy (this Policy) and practices will be implemented;

5.1.3. Privacy roles and responsibilities will be defined and embedded within the Fund;



- 5.1.4. The Fund will remain the responsible party for all Personal Information processed under its control and authority;
- 5.1.5. The Fund will ensure that adequate contracts with operators are concluded where Personal Information is processed by a third-party provider (operator);
- 5.1.6. A Deputy Information Officer will be appointed and be held responsible for addressing all privacy related queries, including queries relating to this Policy; and,
- 5.1.7. A formal privacy training awareness programme will be established and conducted at induction and on an ongoing basis.

## **5.2. Processing limitation**

### **5.2.1. Lawfulness of Processing**

Personal Information will be processed in a lawful manner which does not infringe upon the rights of Data Subjects.

#### *5.2.1.1. Minimality*

Only necessary Personal Information will be collected for a given purpose, and processed only where information is adequate, relevant and not excessive.

#### *5.2.1.2. Consent, justification and objection*

- 5.2.1.2.1. The Fund will ensure that Personal Information is processed only with the necessary consent, or where the Fund has a legitimate business requirement to process Personal Information.
- 5.2.1.2.2. Where consent is not received from the Data Subject, Users will consult with the Deputy Information Officer to determine if Personal Information can be processed.
- 5.2.1.2.3. A valid justification for the Processing of Personal Information will be provided by the Fund to Data Subjects.
- 5.2.1.2.4. Where a Data Subject objects to the Processing of his or her Personal Information, the Fund may no longer process the Personal Information of the Data Subject, unless required to do so in terms of legislation or for legitimate business purposes. In addition, the Data Subject will be informed of the consequences of objection to Processing where these may exist.

#### *5.2.1.3. Collection directly from a Data Subject*

Other than within the lawful exceptions defined by the Act, Personal Information will be collected directly from a Data Subject.

### **5.3. Purpose Specification**

#### **5.3.1. Collection for a specific purpose**

Personal Information will be collected for a specific, explicitly defined and lawful purpose related to a function or business activity of the Fund. All Data Subjects whose Personal Information is collected and processed, will be made aware of the purpose of the collection and Processing of their Personal Information, per the Openness principle in section 5.6 of this Policy.

#### **5.3.2. Retention and restriction of records**

5.3.2.1. Records containing Personal Information will only be retained for as long as necessarily required to achieve the purpose for collection.

5.3.2.2. Users will refer to the Fund's Records Retention Policy in determining the legal requirements for the retention of Records.

5.3.2.3. The Fund will ensure that all Records containing Personal Information are deleted or destroyed when they are no longer required for the purpose collected, or in terms of the stipulated retention period.

5.3.2.4. The destruction or deletion of Records will be performed in a manner that prevents its reconstruction in an intelligible form that allows the identification of a Data Subject. Users will refer to the Fund's Record Retention Policy for approved destruction techniques.

### **5.4. Further Processing Limitation**

5.4.1. Further Processing of a Data Subject's Personal Information will only be permitted if this Processing is compatible with the original purpose of collection and Processing, as defined in Section 5.2 of this Policy.

5.4.2. A process will be implemented to assess whether further Processing of Personal Information is compatible with the original purpose of collection and processing.

5.4.3. If Personal Information is to be used for further Processing, Data Subjects will be informed and provide consent for further Processing.

### **5.5. Information Quality**

5.5.1. The Fund will ensure that all Personal Information held, is complete, accurate, and not misleading.

5.5.2. Data Subjects will be given the opportunity to request the update and correction of their Personal Information on a regular basis.

### **5.6. Openness**

5.6.1. The Fund's PAIA Manual will include details of the Fund's processing operations with regards to Personal Information.

5.6.2. A notice will be provided to Data Subjects at all points of collection of Personal Information.

## **5.7. Security Safeguards**

- 5.7.1. The Fund will ensure the integrity and confidentiality of Personal Information in its possession or under its control by taking appropriate, reasonable, technical and organisational measures to prevent, loss, damage and unauthorised destruction of Personal Information.
- 5.7.2. Users will refer to the Logical Access Control Policy for adequate security safeguards to protect Personal Information.
- 5.7.3. Where there has been a suspected breach of Personal Information or where Personal Information has been accessed by an unauthorised party, Users will contact the Deputy Information Officer immediately.
- 5.7.4. Users will refer to the Privacy Breach Procedure to be followed when a suspected breach occurs.
- 5.7.5. Personal Information will only be processed by operators on behalf of the Fund under the following conditions:
  - 5.7.5.1. All Processing will be with the knowledge and authorisation of the Fund.
  - 5.7.5.2. All Personal Information processed by an operator will be treated as confidential.
  - 5.7.5.3. A written agreement will be in place between the Fund and the operator which requires the operator to have in place reasonable security safeguards to ensure the confidentiality and integrity of Personal Information.
  - 5.7.5.4. There will be a process in place to monitor and report operator compliance with the written agreement.
  - 5.7.5.5. The operator will notify the Fund immediately in the case of any breach of Personal Information.

## **5.8. Data Subject Participation**

- 5.8.1. Upon reasonable request from a Data Subject, the Fund will, as soon as reasonably practical, provide the Data Subject with access to his/her Personal Information. This principle should be considered in conjunction with the information quality condition, addressed in Section 5.5 of this Policy.
- 5.8.2. All formal requests for Records containing Personal Information will be lodged in accordance with the information provided in the Fund's PAIA manual, which is available on the Fund's website.
- 5.8.3. The Fund will take the necessary steps to validate the identity of the Data Subject prior to availing him/her with access to their Personal Information held by the Fund or its operators.

## **5.9. Special Personal Information**

- 5.9.1. Subject to the next paragraph, the Fund may not process any Personal Information of a child, or of a Data Subject concerning their religious or philosophical beliefs, race or



ethnic origin, trade union membership, political persuasion, health or sex life, biometric information, or criminal behaviour.

5.9.2. The Personal Information described in the previous paragraph can only be processed with the explicit consent of the Data Subject, or the parent or guardian of the child, or where the Fund has a legitimate reason to process this Special Personal Information.

5.9.3. In every instance, Users will consult with the Deputy Information Officer to determine whether the Processing of Special Personal Information is permitted.

#### 5.10. **Transborder Information Flows**

The Fund may not transfer Personal Information about their Data Subjects to a third party in a foreign country unless one or all of the following conditions are met:

5.10.1. The Data Subject has provided his or her consent;

5.10.2. The third party is located in a foreign country with adequate data protection legislation;

5.10.3. The transfer is necessary for the performance of a contract;

5.10.4. Children's information may not be transferred trans-border without the written consent of the parent or guardian;

5.10.5. Users are required to consult with the Deputy Information Officer before any trans-border flows of information are performed.

## 6. ROLES AND RESPONSIBILITIES

6.1. The following summarises the responsibilities per stakeholder group related to the application and monitoring of compliance to this Policy:

Stakeholder	Responsibility
Deputy Information Officer	The Deputy Information Officer has been delegated all the responsibilities of the Information Officer as set out below.
Employees and Contractors	Comply with this Policy in relation to the use of and when securing EPPF information and Personal Information.  All Fund employees and contractors must ensure that they comply with this Privacy Policy and instructions issued by the Information Officer, and that the privacy of Data Subjects is respected.
Information Officer	The Information Officer (the Chief Executive) is accountable and responsible for the following: <ul style="list-style-type: none"><li>• Ensuring adequate compliance with the conditions for the lawful Processing of Personal Information;</li><li>• Providing guidance to the Fund and its employees for adequate disclosure of Personal Information, when Special Personal Information can be processed, and providing guidance on Transborder Flows of Personal Information;</li></ul>

Stakeholder	Responsibility
	<ul style="list-style-type: none"> <li>Identifying training requirements and developing a training curriculum in line with legislative and employee requirements;</li> <li>Dealing with Data Subject access requests made in terms of POPIA and PAIA;</li> <li>Monitoring and measuring privacy compliance and enforcement;</li> <li>Responding to breaches and Personal Information incidents;</li> <li>Reporting to management and stakeholders;</li> <li>Performing privacy risk assessments and data inventories;</li> <li>Developing and implementing privacy policies and guidance; and</li> <li>Administering privacy roles and responsibilities.</li> </ul> <p>The Information Officer can delegate all or some of these duties to the Deputy Information Officer.</p>
Head: Information Technology	<p>The Head of the Information Technology department is responsible for the following:</p> <ul style="list-style-type: none"> <li>Ensuring information systems and processes provide adequate protection for Personal Information;</li> <li>Monitoring compliance with the Logical Access Control Policy;</li> <li>Establishing mandatory / standard security requirements for all electronic Personal Information, including encryption of all Personal Information, when necessary.</li> </ul>
Fund Management / Exco	Ensure that appropriate staff structure and authority has been delegated for the execution of this Policy.
Policy Owner	<p>Ensure that the Policy is kept current through the regular review of the Policy.</p> <p>Ensure that policies are made available/communicated to the relevant stake holders.</p> <p>Ensure that deviations from this Policy are documented and sent to the Policy sponsor for approval.</p>
Policy Sponsor	Support the Policy.
Privacy Champion	A Privacy Champion will be appointed within each business unit. The Privacy Champion will be responsible for the implementation, maintenance and monitoring of Privacy compliance within the business unit. The Privacy Champion will report to the Deputy Information Officer in terms of defined Privacy responsibilities and reporting.
Risk and Compliance	Monitor compliance to Policy.



Stakeholder	Responsibility
Internal Audit	Audit according to the approved Policy.

## 7. RELATED INFORMATION AND REFERENCE

7.1. This Policy should be read in conjunction with the following supporting guidelines:

### 7.1.1. Internal Documents:

- 7.1.1.1.Information Classification Policy
- 7.1.1.2.Information Classification Procedure with Information Handling Criteria
- 7.1.1.3.Information Security Policy
- 7.1.1.4.Information Security Standard
- 7.1.1.5.PAIA Manual
- 7.1.1.6.Privacy Standard
- 7.1.1.7.Privacy Breach Management Procedure
- 7.1.1.8.Records Retention and Disposal Policy
- 7.1.1.9.Relevant human resources policies and procedures, including disciplinary procedures

### 7.1.2. External Documents:

- 7.1.2.1.None identified.

### 7.1.3. Regulatory Requirements:

- 7.1.3.1.Protection of Personal act 4 of 2013.
- 7.1.3.2.Promotion of Access to Information Act 2 of 2000.
- 7.1.3.3.Pension Funds Act 24 of 1956.

## 8. EXCLUSIONS

8.1. There are no exclusions to this Policy except when a condition is overridden by another Law.

## 9. REQUEST TO DEVIATE FROM POLICY

9.1. In cases where material and compelling circumstances merit deviation(s) from particular provision(s) of this Policy, written submission shall be sent to the Information Officer, who shall have consider such request in line with the Fund's Governance Framework in whole or in part, or refuse same.

## 10.COMPLIANCE MONITORING

10.1. The implementation of this Policy will be subject to the Fund's compliance monitoring principles.

## **11. NON-COMPLIANCE**

- 11.1. Breaches of this Policy will be seen in a very serious light. Employees who do not conform to the Policy or Principles and Standards will be subject to disciplinary action in terms of the applicable EPPF disciplinary processes and procedures.