SIMEKA

member of Sanlam group

The University of Cape Town Retirement Fund

Data Protection & Privacy Policy

1 July 2021

Prepared by: Simeka Consultants & Actuaries

Table of **Contents**

1. Introduction

The Protection of Personal Information Act (POPIA), which was signed into law in 2013, came fully into effect on 1 July 2020. POPIA gives effect to the constitutional right to privacy by safeguarding Personal Information.

1.1 POPIA mainly intends to

- promote the protection of Personal Information Processed by public and private bodies;
- introduce certain conditions to establish minimum requirements for the Processing of Personal Information;
- provide for the issuing of codes of conduct;
- provide for the rights of persons regarding unsolicited electronic communications and automated decision making.

1.2 The Fund is committed to

- ensuring that all Personal Information will be Processed in a responsible manner that does not unjustifiably infringe the privacy of any Fund Officer or Member;
- securing the integrity and confidentiality of Personal Information of any Fund Officer or Member that comes into its possession or under its control; and
- complying with its obligations in accordance with all applicable and relevant laws including, but not limited to, Data Protection Laws.

2. Definitions

There are three main role players involved:

a) The Fund (which is the Responsible Party in terms of POPIA);
b) The relevant Service Providers (who are the Operators in terms of POPIA); and
c) The Member (who is a Data Subject in terms of POPIA).

"Board"	Means the Board of the Fund as defined in its rules, and for the purposes of POPIA known as the responsible party, who alone or in conjunction with others determine the purpose of and means for Processing Personal Information.
"Consent"	Means any voluntary, specific and informed expression of will, in terms of which permission is given for the Processing of Personal Information.
"Data Protection Laws"	Means any data protection or data privacy laws relating to Personal Information, applicable to the activities of the Fund from time to time (including POPIA) any laws, regulations, guidelines and/or codes of conduct issued by the Information Regulator.
"Data Subject"	Means Fund Members.

"De-identify"	In relation to Personal Information means to delete any information that identifies or can be used or manipulated to identify the Member and Fund Officers, such that it cannot be re-identified again.
"Fund"	Means the University of Cape Town Retirement Fund.
"Fund Officers"	Means the board members, the Principal Officer and the Deputy Principal Officer of the Fund as defined in the rules.
"Information Officer"	Means the individual registered as an Information Officer with the Information Regulator in terms of Data Protection Laws and as reflected in clause 12 of this policy.
"Deputy Information Officer"	Means the individual registered as a Deputy Information Officer with the Information Regulator in terms of the Data Protection Laws as reflected in clause 12 of this policy.
"Information Regulator"	Means the Information Regulator appointed in terms of POPIA.
"IT"	Means information technology.
"Member"	Means for the purposes of this policy, a Member and or beneficiary of the Fund and any data subject for the purposes of POPIA, including Fund Officers if the context relates to the protection of their Personal Information.
"Operator"	Means the Fund's Service Providers.
"Personal Information"	Including, but not limited to: identity and/or passport number; date of birth and age; phone number; email address; online messaging identifier; account number; physical address; gender, race and ethnic origin; photos; marital/relationship status; criminal record; private correspondence; employment history; salary information; financial information; education information; physical and health information including medical history; and membership of organisations/unions; the biometric information of the person; personal opinions, views or preferences of the person; and the name of the person if it appears with other Personal Information relating to the person or if the disclosure of the name itself would reveal information about the person.
"POPIA"	Means the Protection of Personal Information Act, 4 of 2013.
"Process or Processing"	Means any operation or activity or any set of operations, whether by automatic means, in hard copy or digital, 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.
"Responsible Party"	Means the Board.
"Security Event"	Means where there is reason to believe or to suspect that Personal Information has been acquired, disclosed, used, dealt with in any way whatsoever or accessed by an unauthorised party or is reasonably likely to be acquired, disclosed, used or accessed by an unauthorised party.
"Service Provider/s"	Means a Service Provider of the Fund appointed by the Board and for the purposes of POPIA known as an Operator, who Processes Personal Information for the UCTRF in terms of a contract or mandate, without coming under the direct authority of that Responsible Party.
"Special Personal Information"	Means religious or philosophical beliefs; race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information, criminal behaviour to the extent that the information relates to alleged commission by a Member or Fund Officer of any offence or proceedings in respect of any alleged offence by a Member or Fund Officer.

3. Purpose of the Policy

The Fund is committed to the adherence and compliance of POPIA and is committed to ensuring the protection of the Personal Information of Members and Fund Officers. The purpose of this policy is to ensure that the Fund and its Service Providers Process Personal Information responsibly and in a manner that demonstrates their commitment to upholding the right to privacy of Members and Fund Officers, subject to justifiable limitations.

It further establishes a common standard on the appropriate protection of Personal Information of Members and provides general principles regarding the right of individuals to privacy and to reasonable safeguarding and protection of their Personal Information. This policy also specifies minimum requirements and standards that are to be adhered to with regards to the Processing of Personal Information by Service Providers of the Fund.

The Fund may outsource services related to its data protection and IT management to its respective Service Providers.

The Board, however, remains committed to minimising and managing the risks relating to maintaining and protecting all Fund data:

- in accordance with its sensitivity and the risk to which it is exposed; and
- in a manner which is consistent with all relevant legal, regulatory and contractual requirements.

The Board is equally committed to minimising and managing the operational risks that result from the Fund's operations with specific reference to data and IT systems.

The Board, in its commitment to comply with POPIA, requires that the Fund's Service Providers adhere to the lawful Processing of Personal Information in line with POPIA.

4. Scope of the Policy

This policy is applicable to the protection and Processing of Personal Information throughout the information life cycle, from the point of first collection of Personal Information until the time that such information is destroyed or De-Identified. The policy applies to the Fund, its Members, the Board, and all Service Providers contracted with the Fund to deliver various services for the Fund and its Members.

5. Key Principles

The Board will take reasonable steps to ensure lawful Processing of all Personal Information of Fund Officers and Members, taking into account these key principles:

5.1 Accountability

The Fund is accountable for ensuring that the provisions of applicable Data Protection Laws and the requirements outlined in this policy are complied with through implementing appropriate practices, policies and procedures.

5.2 Processing limitation

Information must be adequate, relevant and not excessive and Processed with Consent, unless required in order to comply with legislation. Where Processing is in line with applicable legislation (such as the Pension Funds Act) and the Fund rules, the Fund and Service Providers may Process Personal Information without obtaining prior Consent from Members.

The Fund will only share a Member's Personal Information with Service Providers or third parties if the Member has Consented to such disclosure or to the extent that it is required to do so in terms of its rules, by law, in connection with any legal proceedings or any prospective legal proceedings.

Personal Information should not be retained for longer than is necessary to achieve the purpose for which it is Processed unless authorised or required by applicable laws. Personal information must not be Processed for a secondary purpose unless that secondary purpose is compatible with the original purpose or authorised by Data Protection Laws.

5.3 Purpose

Personal Information must be collected for a specific, explicitly defined and lawful purpose relating to the function or activity of the Fund and notified to the Member or Fund Officer. Where the Fund discloses Personal Information to Service Providers, the Service Providers will be obliged to use that Personal Information only for the reasons and purposes for which it was disclosed.

5.4 Information quality

Personal Information collected must be complete, accurate, not misleading and updated when required, having regard to the purpose for which the information was collected.

5.5 Openness

Members and Fund Officers must be informed of the collection of Personal Information and purpose of collection. This includes that all necessary disclosures as required by applicable Data Protection Laws and this policy are made.

5.6 Security measures

The integrity and confidentiality of Personal Information must be secured and the Board must be comfortable that there are reasonable security safeguards in place against risks such as loss, unauthorised access, destruction, use, amendment or disclosure of Personal Information.

5.7 Data subject participation

A Member or Fund Officer will have the right to request details of any Personal Information held by the Fund in respect of the Member or Fund Officer.

5.8 Special Personal Information

Special Personal Information that is collected or Processed must be treated with the highest of care.

5.9 Sharing of Personal Information

When Personal Information is shared with Service Providers or third parties (including permitting access, transmission or publication), it may only be shared with reasonable assurance that the recipient has suitable privacy and security protection controls in place.

6. Special Personal Information

6.1 Special Personal Information are categories of Personal Information that are afforded a higher level of protection by Data Protection Laws. Particular care should be taken in protecting Special Personal Information from loss, damage, unauthorised use, disclosure or access.

6.2 Subject to any other justifications under Data Protection Laws which may exist in relation to Special Personal Information (or a certain category of Special Personal Information), Special Personal Information should only be Processed and disclosed to Service Providers or third parties with the Consent of the Member (or a competent person in respect of a child).

7. Service Providers

7.1 The Board will ensure that the service agreements with all Service Providers provides that Service Providers Process Personal Information in accordance with this policy and applicable Data Protection Laws.

7.2 The service agreement should take into account the following:

7.2.1 The nature of the Service Provider's services and exposure to the Fund's and Members' Personal Information in terms of Data Protection Laws;

7.2.2 All data pertaining to the Fund and its members must be treated by its Service Providers as confidential and not used for any purpose other than for the performance of any service in terms of the Fund's agreements with the Service Providers and as allowed by any applicable law;

7.2.3 No disclosure to third parties of the Fund's and Members' Personal Information may be made by the Service Providers save to the extent that such disclosure may be required by law, is in line with applicable legislation or with the prior written consent of the Fund;

7.2.4 The Service Providers must put in place a process to ensure that all business-related correspondence and data are officially handed over by any of its exiting employees before their last day of service;

7.2.5 Service Providers must maintain the confidentiality of correspondence sent and received via any medium by ensuring that sensitive Personal Information is correctly addressed, sent only to authorised persons and is password protected where necessary;

7.2.6 Compliance with all relevant laws in respect of the collection, storage, security, destruction and deletion of any record containing Personal Information, for example, information no longer required for the purpose for which it was collected or for which the legal obligations for retention have passed, must, subject to clause 9 of this policy, be destroyed via secure means such as cross-cut shredding (for paper records) or permanent erasure via suitable and agreed mechanisms for electronic records;

7.2.7 Compliance with all policies and procedures pertaining to the protection, privacy, storage, retention, handling, processing and destruction of data, including Personal Information;

7.2.8 Adequate recourse to the Fund, including a right to terminate the agreement, indemnification for breach and/or appropriate insurance cover for cyber security breaches, where the Service Provider is not complying with the requirements set forth in the agreement with the Service Provider;

7.2.9 The requirement to immediately inform the Fund (via the Fund's Information Officer) of any actual or suspected Security Event or compromise to Personal Information in its possession;

7.2.10 The requirement, on the Fund's instructions, via the office of the Fund's Information Officer, to notify the affected Fund Officers or Members and/or the Information Regulator of any actual or suspected Security Event or compromise.

7.3 All Service Providers are required to adhere to POPIA, this policy and all other Data Protection Laws and may, depending on the service they provide to the Fund, be required to declare in writing to the Fund before 1 July 2021 and at a frequency to be determined by the Board thereafter:

7.3.1 How POPIA will generally be adhered to and which security processes and measures are in place to safeguard Personal Information;

7.3.2 In the format as may be prescribed and deemed necessary by the Board, with documentation and/or audit reports, as the case may be, that they:

a) have adequate protection against external system attacks, viruses and any other similar risks;
b) have reliable and comprehensive offsite data protection as part of their disaster recovery plans in place to mitigate the risk of physical destruction of property, information and systems;
c) develop and maintain adequate measures to protect against inappropriate access to systems, data and any other sensitive information through appropriate storage facilities, password requirements, building-entry systems, IT firewalls and other similar processes and/or systems;
d) maintain the necessary cyber insurance to cover a data breach in which Members' Personal Information is stolen by a hacker or cybercriminal.

7.3.3 To minimise the possible risks emanating from a failure or delay in delivering IT processes or information needed for business transactions and operations, the risks of hardware failure, network outages and power outages are addressed to ensure that business as usual can continue with minimal interruption should such events occur;

7.3.4 The impact of a force majeure has been considered as part of their disaster recovery programme to mitigate the risk of not having an appropriate workforce able to access backup systems;

7.3.5 **To minimise the possible risks emanating from the slow or inefficient operation of IT processes supporting business transactions and operations, that they have:**

a) put in place a process to ensure the adequacy and efficiency of their system architecture and capabilities;
b) taken adequate steps to prevent network congestion which can introduce inefficiencies and compromise service delivery;
c) demonstrated the ability to reduce system design inefficiencies and system process inefficiencies where such inefficiencies are identified.

7.3.6 Feedback as to whether they have undergone an ISAE 3402 audit and if so, the results of such audit must be provided to the Fund for consideration at least every 3 years. Service Providers who have not undergone an ISAE 3402 audit must provide written confirmation that their disaster recovery plans and IT systems are sound and that they are tested regularly. Such confirmation should be provided by a third party, such as an external auditor, where possible;

7.3.7 Their compliance to the applicable regulatory requirements regarding the collection and Processing of Personal Information;

7.3.8 Collecting Personal Information is adequate, relevant and not excessive and obtained with Consent, unless required in order to comply with legislation;

7.3.9 Processing Personal Information is done in a manner compatible with the purpose for which it was collected;

7.3.10 Personal Information that is collected or Processed is treated with the highest of care as prescribed by POPIA;

7.3.11 An individual's Consent will only be obtained to process their Personal Information when Personal Information is being collected for reasons other than for legislative or contractual purposes;

7.3.12 Personal Information is kept accurate, complete and up-to-date and reliable for its intended use;

7.3.13 Reasonable security safeguards have been developed and are in place against risks such as loss, unauthorised access, destruction, use, amendment or disclosure of Personal Information;

7.3.14 Personal Information is only shared with third parties where such sharing is compatible with the initial purpose for the Processing and with reasonable assurance that the third party has suitable privacy and security protection controls in place in accordance with Data Protection Laws regarding Personal Information.

7.4 All the Service Providers must confirm annually that they have a disaster data recovery plan in place.

8. Security measures

The Fund, as the Responsible Party, will adopt the following measures and/or procedures to achieve compliance with the provisions of POPIA and any other Data Protection Laws:

8.1 Create and maintain awareness amongst its Fund Officers about its information security policies and procedures through on-boarding processes and ongoing security awareness drives.

8.2 Members and Fund Officers will be informed of the collection of Personal Information and the purpose of collection and be made aware of the rights conferred upon them as data subjects under Data Protection Laws.

8.3 In accordance with the Promotion of Access to Information Act, 2000, the Fund will develop and maintain an access request procedure, which will apply to requests from Data Subjects for access to data under the Data Protection Laws. Such procedure will be documented, made available to Fund Officers and Members and will describe the end-to-end process from the initiation of an access request by a Data Subject, to the execution of such request.

8.4 Where Data Protection Laws prescribe forms for access requests, the Fund will ensure that such forms are placed on their website and are readily available via all Member channels.

8.5 A compliance framework will be developed, implemented, monitored and maintained.

8.6 At a frequency to be determined by the Board, a personal Information impact assessment will be done to ensure adequate measures and standards are in place to comply with the conditions for lawful Processing.

8.7 A general cautionary note will be included in the agendas of meetings of the Board and sub-committees to indicate that the Fund information is “strictly confidential” and that no Personal Information of Members of the Fund and Fund Officers may be made available to third parties other than the contracted Service Providers of the Fund.

8.8 Each Fund Officer must sign a confidentiality undertaking to comply with the provisions of POPIA.

8.9 The participating employers are expected to comply with the provisions of POPIA when dealing with Fund matters and Personal Information of Members and Fund Officers.

8.10 Service Providers:

8.10.1 The provisions in clause 7.2 should be covered in all written agreements with Service Providers;

8.10.2 Declarations in terms of clause 7.3 will be obtained from Service Providers at a frequency to be determined by the Board.

8.11 The Fund will document and implement specific procedures, processes and controls for lodging and handling complaints related to the Processing of Personal Information.

8.12 The Fund will inform Fund Officers and Members of the complaints procedure through their website, member brochures or other documents, which must be readily available and easy to understand. The complaint resolution process must be explained, and contact information for Members to reach the Fund must be provided.

8.13 All Personal Information leaving secure environments is adequately protected by using appropriate technologies, like encryption or physical controls.

8.14 Members' names will be excluded from all generic Fund reports and only Member numbers will be used instead.

8.15 Where specific Member names are needed such as for Pension Funds Adjudicator cases and the distribution of death benefits to beneficiaries, the Fund reports must be clearly marked "strictly confidential".

8.16 All Personal Information that is not relevant to the Board's decision-making must be removed from Fund reports.

8.17 Special care must be taken by Fund Officers and Service Providers to protect the contents of the agenda packs of the Board and sub-committees against unauthorised access.

8.18 Board members will not share Personal Information through unsecure methods and will not transfer Personal Information to a third party in a foreign country.

8.19 All attachments containing Personal Information of Members or Fund Officers must be password protected before it is sent via email to any person.

8.20 Special care must be taken when disposing of used Fund documents and these documents must be destroyed in a controlled environment.

8.21 Where a Fund Officer becomes aware or suspicious of any Security Event such as any 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.

8.22 Where there are reasonable grounds to believe that a Security Event has occurred and to the extent required by applicable laws, the Fund will ensure that the Information Regulator and the affected Fund Officers or Members (unless the identity of the data subjects cannot be established) are notified as soon as is reasonably possible.

9. Data and Storage retention

9.1 The Fund and/or its Service Providers will ensure that Personal Information, including Special Personal Information which they Process, is Processed (including captured, used, disclosed, stored and destroyed) in a secure and confidential manner appropriate to the classification of the information, in accordance with the relevant provisions of Data Protection Laws.

9.2 In order to comply with Data Protection Laws, the Fund and its Service Providers:

9.2.1 Must keep record of the Personal Information it has collected, including correspondence or comments in an electronic or hardcopy file format. Personal Information may be Processed for as long as is necessary to fulfil the purposes for which that Personal Information was collected and/or as permitted or required by applicable law;

9.2.2 **May retain Personal Information for longer periods for statistical, historical or research purposes, and should this occur, the Fund and/or its Service Providers will ensure that appropriate safeguards have been put in place to ensure that:**

(i) all recorded Personal Information will continue to be Processed in accordance with this policy and the applicable laws; and

(ii) the records of Personal Information shall not be used for any other purposes.

9.2.3 Must, once the purpose for which the Personal Information was initially collected and Processed no longer applies or becomes obsolete, and there is no legitimate reason for retention of such Personal Information, ensure that it is deleted, destroyed or De-Identified.

9.3 Where the Fund and its Service Providers no longer need Personal Information for achieving the purpose for which it was initially collected or subsequently Processed, but they retain such Personal Information for the purposes of proof, the Fund and its Service Providers will not be required to delete or destroy such information, but must restrict the Processing of such Personal Information from further circulation, publication or use and ensure that there are appropriate security safeguards in place that are consistent with the requirements of this policy in respect of such Personal Information.

10. Access and correction of Personal Information

Members and Fund Officers have the right to access the Personal Information that the Fund and its Service Providers hold about them. Members and Fund Officers also have the right to request the Fund and its Service Providers to update or correct their Personal Information, if self-service access is not available to them. The Fund and its Service Providers must take all reasonable steps to confirm a Member's identity before providing details of their Personal Information or making changes to their Personal Information.

11. Complaints Procedures

The Fund's complaints procedure described in clauses 8.11 and 8.12 must, at a minimum, contain the following:

11.1 Members must be encouraged to submit their complaints/enquiries, which relate to the Processing of Personal Information, directly to the Fund instead of approaching the Information Regulator, in order to give the Fund the opportunity to swiftly and efficiently address the complaint/enquiry internally and outside of the public domain.

11.2 A Member or Fund Officer must be able to direct a challenge regarding an alleged infringement of their rights to the Fund's Information Officer. The Fund must therefore establish procedures to receive and respond to enquiries or challenges to its policies and practices relating to the handling of Personal Information. These procedures must be easily accessible and simple to use.

12. Information Officers

12.1 The Fund must appoint an Information Officer.

12.2 The Fund may, at its own discretion, appoint a Deputy Information Officer who will assist the Information Officer in fulfilling his/her responsibilities.

12.3 The Information Officer's duties and responsibilities must be set out in a written agreement.

13. Monitoring and enforcing

13.1 The Board is responsible for monitoring and overseeing the implementation of this policy.

13.2 Non-compliance with this policy may result in possible termination of mandates of Service Providers and disciplinary action against Fund Officers.