NOVEMBER 2022

CPUT RETIREMENT FUND

("the Fund")

CONFIDENTIALITY POLICY

---

1. Purpose

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

2. Introduction

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

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

As such, it is necessary to set out how these imperatives (transparency and confidentiality within the required legislative context) may be reconciled in a way which reflects good governance. Board Members and associated Fund parties are expected to comply with the contents of this policy – Board Members, the Principal Officer and Deputy Principal Officer will be required to commit in writing to compliance with the policy.

2.2. This policy sets out:-

2.2.1. What information of the Fund is confidential;

2.2.2. The circumstances in which a Board Member or associated Fund party is entitled to have access to confidential information;

2.2.3. The circumstances in which confidential information may be utilised and the relevant POPIA exceptions;

2.2.4. The obligation to ensure the protection of the fund's confidential information; and

2.2.5. The best practices to be adopted with respect to data confidentiality and compliance with the POPIA.

2.3. This policy must be read in conjunction with the Communication Policy and the Code of Conduct of the Fund.

2.4. "Personal information" is very widely defined under the POPIA and means information relating to identifiable, living, natural persons and identifiable, currently existing, juristic persons (legal entities). "Personal information" includes (but is not limited to) such items as gender, race, age, disability, language, "medical, financial, criminal or employment history", and contact details including e-mail address and phone numbers.

2.5. Under the requirements of the POPIA, there are eight separate conditions for the lawful processing of Personal Information (by or on behalf of a Responsible Party). These conditions, briefly, include:

- *"Accountability"*: A Responsible Party must comply with the provisions of the Act and supporting legislation (e.g. the Regulations to the Act) when planning how and why to process personal information, and when actually processing it.

- *"Processing limitation"*: Personal Information must be processed in a lawful manner and only for its given purpose – the Personal Information obtained must not be excessive in relation to the purpose for which it is processed. It should also not infringe on the privacy of the data subject. Consent must be obtained from the data subject except in specified circumstances (refer to paragraph 4.4 below).

- *Purpose specification*: Personal Information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the Responsible Party. Records of Personal Information may be retained for a required period of time, "for historical, statistical or research purposes if the Responsible Party has established appropriate safeguards against the records being used for any other purposes".

- *Further processing limitation*: Any further processing of information must be compatible with the original purpose.

- *Information quality*: A Responsible Party must take reasonable steps to ensure that Personal Information is complete, accurate, not misleading, and updated where necessary (and having regard to the purpose for which Personal Information is collected).

- *"Openness" (transparency)*: A Responsible Party must document the processing operations under its responsibility and must generally take reasonable steps to ensure that the data subjects are aware of the information being collected and the purpose thereof.

- *Security safeguards*: A Responsible Party must secure the integrity and confidentiality of Personal Information in its possession or under its control by taking appropriate technical and organisational measures to prevent loss of data or unlawful access, and must also employ regularly updated safeguards against any internal or external risks.

- *Data subject participation*: A data subject has the right, under the Promotion of Access to Information Act (PAIA), to request a Responsible Party to confirm whether or not the Responsible Party holds personal information about the data subject, to confirm whether corrections should be made to the information in question, and to be provided with details of all third parties with whom the data has been shared.

In addition to the above, special provisions also apply to the processing Personal Information of children (natural persons under the age of 18 years), where consent would be required unless certain explicit conditions apply (refer to paragraph 4.4 below). Additional conditions under the POPIA apply to "special personal information" (religion, politics, "race or ethnic origin", health matters, sexuality, criminal record, etc.). The Fund will strive to meet all of these conditions and provisions, subject to any allowable exclusions.

2.6. In accordance with the POPIA, the Fund will appoint a designated Information Officer. The Information Officer's responsibilities include the encouragement of compliance with the conditions for the lawful processing of personal information, dealing with requests made pursuant to the POPIA, working with the Information Regulator where applicable, and otherwise ensuring compliance with the provisions of the Act.

2.7. For the purposes of this policy, "confidential information" excludes information which is in the public domain. However, a Board Member or Fund related party who asserts that information is not confidential because it is in the public domain, bears the onus of demonstrating that such information is in fact in the public domain. In addition, Board members and Fund related parties should bear in mind that information such as addresses and telephone numbers which are in the public domain are still "Personal Information" as defined in and protected by the POPIA.

3. What Information is Confidential?

3.1. The confidential information of the Fund can be categorised as follows:

Nature of the information	Access to the information
Board information, being • minutes of meetings of the Board and any Board subcommittee; • advice received by the Board or any Board subcommittee from the service providers to the Fund (including legal advice whether or not in contemplation of litigation); • any advice provided by a service provider to the Fund in its capacity as such; • any reporting of any nature received by the Board or any Board subcommittee; • any Board appraisal; • any correspondence to or from any Board Member, Principal Officer, or associated Fund party;	A Board Member or Board subcommittee member has access to all the Board information referred to, including all such relevant Board information prior to that Board Member or Board subcommittee member taking office. This information is not to be disseminated to non-Fund parties in any form unless it is in accordance with a legal requirement and/or has been agreed to by the wider Board and, where applicable, agreed to by the service provider responsible for the information (or to whom the information pertains). For associated Fund parties, including service providers, this information may only be accessed should it be required for the

• any personal information of a Board Member or person who is nominated or proposed as a Board Member; and • any other information relating to the Board, a Board subcommittee or a Board Member which by its nature is confidential or which the Board or a subcommittee categorises as confidential.	successful completion of actions or services required by the Fund in terms of any contractual agreement and/or falls within the scope of a legislative requirement, and does not infringe on the rights of any other service provider or Fund party. This applies with the exception of any information or details which may be deemed by the Board to be sensitive information and as such should not be disclosed to all or specific Fund parties.
Any **information** of whatsoever nature relating to, and/or correspondence with, a **current or former member**, and his or her **dependants** or **beneficiaries**, which is in the possession of the Fund, any of its service providers, or any other associated Fund party, whether or not this is in order to carry out services required by the Fund. This specifically includes any data relating to a Fund member.	A Board Member or Board subcommittee member has access to the information, and/or correspondence with, a current or former member, and his or her dependants or beneficiaries, only if there is an issue which the Board or subcommittee must decide in relation to that current or former member, or his or her dependants or beneficiaries, such as the quantum of a benefit payable, or how a benefit is to be paid, or in respect of a dispute relating to a benefit or a right to a benefit. A Board Member is **not** entitled to information relating to a current or former member, or his or her dependants or beneficiaries, merely out of interest, or which does not fall within the specific requirements set out above. Associated Fund parties, including service providers, have access to the information, and/or correspondence with, a current or former member, and his or her dependants or beneficiaries, or only where

	such information is necessary to successfully perform any duties or actions required by and agreed with the Fund. Although the consent of the individual concerned (or the responsible person in the case of minor children) will not normally be required, any Personal Information relating to such individuals must be collected, held and processed for a specific, explicitly defined and lawful purpose and must not be excessive in relation to the purpose for which it is processed.
Any information relating to an **employer** which participates, or former employer which previously participated, in the Fund, and which is held by the Fund, or any of its service providers, or any other Fund related party, whether or not this is in order to carry out services required by the Fund.	A Board Member or any associated Fund party is only entitled to the information and correspondence referred to, to the extent that this is necessary to resolve any issue which has arisen or to perform any required action in respect of the employer.
Any information relating to the **operation of the Fund**, being: • the details of its contractual arrangements; • any litigation or judicial or quasi-judicial process in which the Fund is involved; • all correspondence between the Fund, its service providers, any other associated Fund parties, or any other person; • the technical know-how, operational arrangements or proprietary information, whether it has a commercial value or not, of any current or former service provider to the Fund; • the details of any bank account operated by the Fund or any service provider on behalf of the Fund;	A Board Member or Board subcommittee member (to the extent that it is relevant to their responsibilities) is entitled to any information relating to the operation of the Fund as set out here. This information is not to be disseminated to non-Fund parties in any form unless it is in accordance with a legal requirement and/or has been agreed to by the Board and, where applicable, agreed to by the service provider responsible for the information (or to whom the information pertains). For all other associated Fund parties, including service providers, this information may only be accessed should it be required for the

• the details of any product or investment arrangement in which the Fund is invested; and • the personal details of any current or former Board Member or employee, the Principal Officer and Deputy Principal Officer of the Fund, or any service provider to the Fund.	successful completion of actions or services required by the Fund in terms of any contractual agreement, and/or falls within the scope of a legislative requirement, and does not infringe on the rights of any other service provider or Fund party. This applies with the exception of any information or details which may be deemed by the Board to be sensitive information and as such should not be disclosed to all or specific associated Fund parties.
Any **other information** in the possession of the Fund which the Board or any subcommittee categorises as confidential.	Notwithstanding the provisions above, the Board may at any time determine that any confidential information may not be provided to or accessed by any Board Member or any other associated Fund party; and in that event must provide reasons for that to that Board Member or associated Fund party.

4. Disclosure of Confidential Information

4.1. No Board Member or associated Fund party, including service providers, may disclose any confidential information of the Fund to any person who does not have a right to such confidential information. In the event that a Board Member or associated Fund party does (whether intentionally or accidentally) disclose confidential information of the Fund to a person who does not have a right to that confidential information, and this disclosure was not in accordance with an instruction received from the Board or an authorised Fund representative such as the Chairperson of the Fund or the Principal Officer, then that Board Member or associated Fund party must notify the Chairperson of the Board immediately thereof and also make a disclosure of this to the Board as soon as possible.

4.2. No Board Member or associated Fund party, including service providers, may allow confidential information in his / her / their possession to be accessed by any person / entity who has no lawful right to such confidential information. Although a Board Member or associated Fund party may not

be able to prevent a person obtaining unlawful access to such confidential information, each Board Member or associated Fund party must take care to ensure that, as far as is reasonably possible, any confidential information in his or her possession is safe-guarded and protected. Thus, confidential information in documentary form should not be left lying around where unauthorised persons may have sight of it or be able to access it.

Furthermore, in accordance with the POPIA, Responsible Parties and Operators (including Board Members and the Principal Officer) must secure the integrity and confidentiality of Personal Information in their possession or under their control by taking appropriate technical and organisational measures to prevent loss or unlawful access of such information, and must also employ regularly updated safeguards against any internal or external risks. This extends to measures to ensure the security of such information held on personal communication devices such as smartphones, tablets and laptop computers, as well as information held in documentary (paper) form.

4.3. Each Board Member or associated Fund party must not allow any third party to be able to access confidential information of the Fund for the financial advantage, or any other advantage, which the person accessing such information may derive therefrom. For example, a Board Member may not allow any member data to be accessed by a financial services provider with a view to such financial services provider generating business therefrom, unless the member whose data is so released has consented in writing to that.

4.4. In accordance with section 11 of POPIA, the consent of the data subject (the member) is not required if the Personal Information is being used to comply with “an obligation imposed by law on the responsible party” (the Fund) and/or to “protect a legitimate interest of the data subject”. The Board considers that member consent is not required because the Fund and its service providers are obliged to process the members’ relevant Personal Information in order to comply with the Pension Funds Act, and also to protect the legitimate interest (the rights) of members as members of the Fund.

Similarly, the consent of a “competent adult” (parent, guardian or caregiver) is not required if the Personal Information of children is being used “for the establishment, exercise or defence of a right or obligation in law” (Section 35(1)). The Board considers that such consent is not required because the Fund and its service providers are processing the child’s relevant Personal Information in order to establish and protect the possible rights of the child as a beneficiary, in death-in-service cases.

Personal information about a deceased person is not considered Personal Information as defined in the POPIA (although personal information relating to dependants and/or possible beneficiaries of deceased Fund members is clearly protected by POPIA).

5. Duty to Protect Confidential Information

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

5.1.1. Each service provider to the Fund must be required to take steps to ensure that the personal information (and any other confidential information) relating to the Fund and its members is processed in accordance with the POPIA requirements, and is not accessed unlawfully by any third party, or used for any purpose (whether or not for any financial or other advantage by that service provider or any third party) other than for the purpose for which it is held to provide benefits to the fund membership or to render services to the Fund;

5.1.2. Personal information (and any other confidential information) relating to the Fund and its members, that is held by a service provider, is subject to the retention requirements set out in the POPIA and must, on the termination of the mandate given by the Fund to that service provider, be returned to the Fund, destroyed or retained in the safe custody of that service provider for the benefit of the Fund for such period specified by the Fund (which may be indefinitely so as to protect any legitimate interests, to the extent that this is compatible with the POPIA retention requirements), or any combination of these, in each case as determined by the Board; and

5.1.3. The Board must ensure that the confidential information of the Fund is stored in a way that will be accessible in the future, unless the Board is reasonably certain that the retention of such confidential information does not, and never will, serve any practical purpose.

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

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

6.1.1. Password protection should be applied to all electronically distributed Fund documents when such documentation may contain sensitive or member related information. Passwords should be changed regularly and should be communicated separately (e.g. by WhatsApp or SMS), i.e. passwords should not be sent with the documents themselves.

6.1.2. Where practically possible, member information should be suitably “de-identified” in Fund documentation unless the identifying information is necessary in the context of a required decision, is required to comply with a legal obligation, or is needed to protect the legitimate interest of a data subject.

6.1.3. "Hard" copies (i.e. printed copies) of any Fund documentation must be limited to the extent possible, since these may be easily intercepted or misplaced. If hard copies containing members' personal information are distributed in a meeting, best practice would normally be to collect and destroy these at the end of the meeting. The Fund should avoid the practice of circulating hard copies of documents such as "agenda packs", where these include members' personal information, in advance of meetings – best practice is to circulate such documents in password-protected electronic form.

6.1.4. Personal email addresses that are not approved by the Fund as well as personal electronic devices that are not approved by the Fund are not to be utilised for the review, processing, or manipulation of any Fund related information. Board Members or other parties who wish to (or need to) make use of personal email addresses and personal devices should seek prior approval from the Fund. Board Members (and other parties where relevant) must take personal responsibility for the encryption of devices and the security of passwords and email accounts, noting that a "data breach" must be reported to the Board and then to the Information Regulator as well as the affected members, as noted in paragraph 6.1.7.

6.1.5. All Fund parties are not to allow any external non-Fund parties (e.g. family members, colleagues, friends) to access devices with Fund information.

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

6.1.7. All Fund parties to review the suitability of security levels on electronic devices used for Fund and related information, and security levels applying to e-mail accounts and electronic data storage, so as to ensure compliance with this policy. Board Members are required to accept personal responsibility in this regard.

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

By their signature the Board hereby approve the Confidentiality Policy as set out above.

24 November 2023

Chairperson Date

24 November 2023

Principal Officer Date