Annexure A

Glossary

TERM	ACRONYM	DEFINITION
Biometrics	--	A technique of personal identification that is based on physical, physiological or behavioural characteristics including blood type, fingerprints, DNA analysis, retinal or iris scanning, and voice recognition.
Breach	--	A confirmed incident in which personal information was compromised, lost, destroyed, altered, and/or exposed to or processed by unauthorised individuals or entities, and which requires notification procedures in terms of our contractual obligations and/or POPIA.
Child	--	A person under the age of 18 years who is not legally competent to take any action or decision in respect of him- or herself without the assistance or consent of a parent, guardian or similar competent person.
Confidentiality	--	The information security principle that information is not made available or disclosed to unauthorised individuals or entities.
Consent	--	Any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
Control	--	A measure put in place to manage risk.
Data Subject	--	A natural person (individual) or juristic person (legal entity) to whom personal information relates or who can be identified by such information.
De-identify	--	Delete or destroy personal information that identifies a data subject, can be used or manipulated to identify them, or that can be linked to other information that identifies them.
Direct marketing	--	To approach a data subject (in person, by mail, or by electronic communication) for the purpose of promoting or offering to supply goods or services, or to request a donation of any kind for any reason.
Effective date	--	The date from which this policy becomes implementable and enforceable.
Guidelines	--	Information or advice on how to act or the controls that should be used in a specific scenario or situation, covering recommendations or best practice to provide additional detail or further context. Guidelines are typically recommended but not mandatory.
Incident	--	An identified occurrence of an adverse event, indicating a breach of policy, control failure, or previously unknown situation that may have an impact on the privacy or data protection responsibilities of the organisation. Some incidents may become breaches once confirmed or investigated.
Information Officer	IO	An individual contemplated by POPIA and PAIA who is responsible for implementing and overseeing measures to give effect to the conditions for the lawful processing of personal information, and ensuring that the organisation complies with its obligations in terms of POPIA and PAIA.
Information Regulator	IR	The regulatory body established by section 39 of POPIA, and who has oversight and authority over POPIA and PAIA.
Integrity	--	The information security principle that describes the accuracy and completeness of information, and the assurance that it is not compromised by unauthorised modification.
Minimality	--	The use of only the smallest subset of personal information needed to perform and activity, fulfil a duty, or achieve a purpose related to its collection.
Operator	--	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, i.e. a person or organisation that is a separate legal entity to the Fund.

TERM	ACRONYM	DEFINITION
--	**PAIA**	The Promotion of Access to Information Act 2 of 2000, as amended, and its Regulations.
Personal Information	PI	As defined by POPIA, personal information is information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to— (a) 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, conscience, belief, culture, language and birth of the person, (b) information relating to the education or the medical, financial, criminal or employment history of the person, (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person, (d) the biometric information of the person, (e) the personal opinions, views or preferences of the person, (f) 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, (g) the views or opinions of another individual about the person, and (h) 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.
Processing	--	Any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including— (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use, (b) dissemination by means of transmission, distribution or making available in any other form, or (c) merging, linking, as well as restriction, degradation, erasure or destruction of information.
Public body		Means- *a)* any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or *b)* any other functionary or institution when— (i) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or exercising a public power or performing a public function in terms of any legislation.

TERM	ACRONYM	DEFINITION
Record	--	Any recorded information— (a) regardless of form or medium, including any of the following: (i) Writing on any material, (ii) 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, (iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means, (iv) book, map, plan, graph or drawing, (v) 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. (b) in the possession or under the control of a responsible party (c) whether or not it was created by a responsible party, and (ii) (d) regardless of when it came into existence.
Responsible Party	RP	A public or private body who alone, or in conjunction with others, determines the purpose of and means for processing personal information.
Restriction	--	To withhold from circulation, use or publication and personal information, but not to delete or destroy such information.
Risk	--	A measure of the extent to which personal data and information is threatened by a potential event, circumstance or occurrence.
Special personal information	**SPI**	As defined by POPIA, more sensitive categories of personal information which may not be processed unless certain conditions are met and/or more stringent security controls are applied, including: (a) religious or philosophical beliefs, (b) race or ethnic origin, (c) trade union membership, (d) political persuasion, (e) health or sex life, (f) biometric information, (g) the criminal behaviour of a data subject to the extent that such information relates to the alleged commission by a data subject of any offence, or any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings, and (h) the personal information of children.
Standards	--	A document that provides specific and more detailed mandatory controls that help to enforce and support policies, establishing the minimum requirements necessary to drive consistent embedding and behaviour. Standards may be based on external best or acceptable practice or an internal view of minimum requirements.
Third party service provider	--	See definition for “Operator”.