THE NAL'IBALI TRUST
PERSONAL INFORMATION PROTECTION POLICY

1. Introduction

This Policy sets out the obligations of The Nal'ibali Trust, an Organisation registered in South Africa under Registration number IT547/2016, whose registered office is at 2 Dingle Avenue, Corner Rosmead Avenue, Kenilworth, 7708 ("the Organisation") regarding the protection of personal information and the rights of employees, customers, business contacts, etc. ("data subjects") in respect of their personal information under The Protection of Personal Information Act or "POPIA". "The Protection of Personal Information Act" means legislation and regulations in force from time to time regulating the use of personal information.

This Policy sets the Organisation's obligations regarding the collection, processing, transfer, storage, and disposal of personal information. The procedures and principles set out herein must be followed at all times by the Organisation, its employees, agents, contractors, or other parties working on behalf of the Organisation.

2. Definitions

"consent"	means any voluntary, specific and informed expression of will in terms of which permission is given to the processing of personal information;
"responsible party"	means the natural or legal person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal information. For the purposes of this Policy, the Organisation is the responsible party for all personal information relating to data subjects such as employees, customers, business contacts, etc. used in our business for our commercial purposes;
"operator"	means a natural or legal person or organisation which processes personal information on behalf of a responsible party;
"data subject"	means a living identifiable natural person or existing juristic person about whom the Organisation holds personal information;
"personal information"	Means any 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, nationality, 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;
"personal information breach"	means a breach of security leading to the accidental or unlawful disclosure of, access to, or use of personal information under the control of the Organisation;
"processing"	means any operation or set of operations performed on personal information or sets of personal information, whether or not by automated means, such as but not limited to the collection, receipt, recording, organisation, structuring, storage, adaptation / alteration, retrieval, use, disclosure by transmission/dissemination or otherwise making available, alignment, merging, linking/combining, restriction, erasure or destruction thereof.
"de-identify"	means to delete any information that— (a) identifies the data subject;

	(b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or (c) can be linked by a reasonably foreseeable method to other information that identifies the data subject.
"special personal information"	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 (b) the criminal behaviour of a data subject to the extent that such information relates to— (i) the alleged commission by a data subject of any offence; or (ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

3. Scope

3.1 The Organisation is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal information, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

3.2 The Organisation's Information Officer is the person at the head of the Organisation or the person acting in that position or the person duly appointed by the person at the head of the business. The Information Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

3.3 The Organisation's Information Officer has appointed a Deputy Information Officer that will assist him/her with ensuring compliance with the Protection of Personal Information Act. The most recent details of the Information Officer and appointed deputy can be obtained from the Human Resources Department.

3.4 All employees that are appointed in positions with an inherent function of the supervision of others and/or performance of a department/division/unit are responsible for ensuring that all employees, agents, contractors, or other parties working on behalf of the Organisation comply with this Policy and, where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance.

3.5 Any questions relating to this Policy or to POPIA should be referred to the Information Officer or the Deputy Information Officer. In particular, the Information Officer or the Deputy Information Officer should always be consulted in the following cases:

a) if there is any uncertainty relating to the lawful basis on which personal information is to be collected, held, and/or processed;

b) if consent is not being relied upon in order to collect, hold, and/or process personal information;

c) if there is any uncertainty relating to the retention period for any particular type(s) of personal information;

d) if any new or amended Privacy Notices or similar privacy-related documentation are required;

e) if any assistance is required in dealing with the exercise of a data subject's rights (including, but not limited to, the handling of data subject access requests);

f) if a personal information breach (suspected or actual) has occurred;

g) if there is any uncertainty relating to security measures (whether technical or organisational) required to protect personal information;

h) if personal information is to be shared with third parties (whether such third parties are acting as third-party service provider or operators);

i) if personal information is to be transferred outside of South Africa and there are questions relating to the legal basis on which to do so and legislation, binding corporate rules or agreements that protects such personal information in third party countries;

j) when any significant new processing activity is to be carried out, or significant changes are to be made to existing processing activities, which will require a POPIA Impact Assessment;

k) when personal information is to be used for purposes different to those for which it was originally collected;

l) if any automated processing, including profiling or automated decision-making, is to be carried out; or

m) if any assistance is required in complying with the law applicable to direct marketing by means of electronic communication.

4. The Protection of Personal information Principles

This Policy aims to ensure compliance with POPIA and sets out the following principles with which any party handling personal information must comply with. Responsible Parties are responsible for, and must be able to demonstrate, such compliance. All personal information must be:

4.1 processed lawfully, fairly, and in a transparent manner in relation to the data subject;

4.2 collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest for historical,

research or statistical purposes shall not be considered to be incompatible with the initial purposes;

4.3 adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;

4.4 accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal information that is inaccurate, having regard to the purposes for which it is processed, is erased/destroyed, or rectified without delay;

4.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal information is processed. Personal information may be stored for longer periods insofar as the personal information will be processed solely for archiving purposes in the public interest such as for historical, statistical or research purposes, subject to implementation of the appropriate safeguards to prevent such records from being used for any other purpose;

4.6 processed in a manner that ensures appropriate security of the personal information, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

5. The Rights of Data Subjects

POPIA sets out the following key rights applicable to data subjects:

5.1 The right to be informed;

5.2 the right of access;

5.3 the right to rectification;

5.4 the right to erasure (also known as the ‘right to be forgotten’);

5.5 the right to restrict processing;

5.6 the right to object; and

5.7 rights with respect to automated decision-making and profiling

5.8 rights with respect to direct marketing using electronic communication as medium.

6. Lawful, Fair, and Transparent Data Processing

6.1 POPIA seeks to ensure that personal information is processed lawfully without adversely affecting the rights of the data subject. Specifically, the processing of personal information shall be lawful if at least one of the following applies:

a) the data subject has given consent to the processing of their personal information for one or more specific purposes;

b) the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;

c) the processing is necessary for compliance with a legal obligation to which the responsible party is subject;

d) the processing is necessary to protect the legitimate interests of either the data subject, the responsible party or a third party to whom such information is supplied; or

e) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the responsible party; or

6.2 If the personal information in question is special category personal information (also known as “special personal information”), at least one of the following conditions must be met:

a) the data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless the law prohibits them from doing so);

b) the processing is necessary for the purpose of establishment, exercise or defence of a right or obligation in law;

c) processing is required to serve an obligation in public or international law;

d) the processing relates to special personal information which is deliberately made public by the data subject;

e) the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;

f) the processing is authorised by the Information Regulator upon successful application; or

g) the processing is necessary for archiving purposes in the public interest for historical, research or statistical purposes.

7. Consent

If consent is relied upon as the lawful basis for collecting, holding, and/or processing personal information, the following shall apply:

7.1 Consent is a clear indication, as far as possible in writing, by the data subject that they agree to the processing of their personal information. Silence, pre-ticked boxes, or inactivity do not amount to consent.

7.2 Where consent is given in a document which includes other matters, the section dealing with consent must be kept clearly separate from such other matters.

7.3 Data subjects are free to withdraw consent at any time and it must be made easy for them to do so. If a data subject withdraws consent, their request must be honoured promptly, unless such withdrawal of consent will significantly adversely affect the responsible party.

7.4 If personal information is to be processed for a different purpose that is

incompatible with the purpose or purposes for which that personal information was originally collected that was not disclosed to the data subject when they first provided their consent, consent to the new purpose or purposes may need to be obtained from the data subject.

7.5 If special personal information is processed, the Organisation shall normally rely on a lawful basis other than explicit consent. However, if explicit consent is relied upon, the data subject must do so in writing.

7.6 In all cases where consent is relied upon as the lawful basis for collecting, holding, and/or processing personal information, records must be kept of all consents obtained in order to ensure that the Organisation can demonstrate its compliance with consent requirements.

8. Specified, Explicit, and Legitimate Purposes

8.1 The Organisation collects and processes the personal information set out in Part 23 of this Policy. This includes:

a) personal information collected directly from data subjects; or

b) personal information obtained from third parties.

8.2 The Organisation only collects, processes, and holds personal information for the specific purposes set out in Part 23 of this Policy (or for other purposes expressly permitted by POPIA).

8.3 Data subjects must be kept informed at all times of the purpose or purposes for which the Organisation uses their personal information. Please refer to Part 15 for more information on keeping data subjects informed.

9. Adequate, Relevant, and Limited Processing

9.1 The Organisation will only collect and process personal information for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 8, above, and as set out in Part 23, below.

9.2 Employees, agents, contractors, or other parties working on behalf of the Organisation may collect personal information only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal information must not be collected.

9.3 Employees, agents, contractors, or other parties working on behalf of the Organisation may process personal information only when the performance of their job duties requires it. Personal information held by the Organisation cannot be processed for any unrelated reasons.

10. Accuracy of Personal Information / Keeping Up to Date

10.1 The Organisation shall ensure that all personal information collected, processed, and held by it is kept accurate and up to date. This includes, but is not limited to, the rectification of personal information at the request

of a data subject, as set out in Part 17, below.

10.2 The accuracy of personal information shall be checked when it is collected and, as determined by each Line manager, as and when required, having due regard to the nature and purpose of the personal information.

10.3 If any personal information is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

11. Retention of Personal Information

11.1 The Organisation shall not keep personal information for any longer than is necessary in light of the purpose or purposes for which that personal information was originally collected, held, and processed.

11.2 When personal information is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

11.3 For full details of the Organisation's approach to data retention, including retention periods for specific personal information types held by the Organisation, please refer to our Personal Information Retention Policy.

12. Secure Processing

12.1 The Organisation shall ensure that all personal information collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 25 to 30 of this Policy.

12.2 All technical and organisational measures taken to protect personal information shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal information.

12.3 Data security must be maintained at all times by protecting the confidentiality, integrity, and availability of all personal information as follows:

a) only those with a genuine need to access and use personal information and who are authorised to do so may access and use it;

b) personal information must be accurate and suitable for the purpose or purposes for which it is collected, held, and processed; and

c) authorised users must always be able to access the personal information as required for the authorised purpose or purposes.

13. Accountability and Record-Keeping

13.1 The Information Officer is responsible for administering this Policy and

for developing and implementing any applicable related policies, procedures, and/or guidelines.

13.2 The Organisation shall follow a “privacy by design” approach at all times when collecting, holding, and processing personal information. POPIA Impact Assessments shall be conducted if any processing presents a significant risk to the rights of data subjects (please refer to Part 14 for further information).

13.3 All employees, agents, contractors, or other parties working on behalf of the Organisation shall be given appropriate training in the protection of personal information, addressing the relevant aspects of POPIA, this Policy, and all other applicable Organisation policies.

13.4 The Organisation’s protection of personal information compliance shall be regularly reviewed and evaluated by means of POPIA Audits.

13.5 The Organisation shall keep written internal records of all personal information collection, holding, and processing, which shall incorporate the following information:

a) the name and details of the Organisation, its Information Officer, and any applicable operators with whom personal information is shared;

b) the purposes for which the Organisation collects, holds, and processes personal information;

c) the Organisation’s legal basis or bases (including, but not limited to, consent, the mechanism(s) for obtaining such consent, and records of such consent) for collecting, holding, and processing personal information;

d) details of the categories of personal information collected, held, and processed by the Organisation;

e) details of any transfers of personal information outside of South Africa including security safeguards;

f) details of how long personal information will be retained by the Organisation (please refer to the Organisation’s Personal Information Retention Policy);

g) details of personal information storage, including location(s);

h) detailed descriptions of all technical and organisational measures taken by the Organisation to ensure the security of personal information.

14. The POPIA Impact Assessments and Privacy by Design

14.1 In accordance with the privacy by design principles, the Organisation shall carry out POPIA Impact Assessments for any and all new projects and/or new uses of personal information which involve the use of new technologies and where the processing involved is likely to result in a high risk to the rights of data subjects.

14.2 The principles of privacy by design should be followed at all times when collecting, holding, and processing personal information. The following factors should be taken into consideration:

a) the nature, scope, context, and purpose or purposes of the collection, holding, and processing;

b) the state of the art of all relevant technical and organisational measures to be taken;

c) the cost of implementing such measures; and

d) the risks posed to data subjects and to the Organisation, including their likelihood and severity.

14.3 The protection of POPIA Impact Assessments shall be overseen by the Information Officer or the Deputy Information Officer and shall address the following:

a) the type(s) of personal information that will be collected, held, and processed;

b) the purpose(s) for which personal information is to be used;

c) the Organisation's objectives;

d) how personal information is to be used;

e) the parties (internal and/or external) who are to be consulted;

f) the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

g) risks posed to data subjects;

h) risks posed both within and to the Organisation; and

i) proposed measures to minimise and handle identified risks.

15. Keeping Data Subjects Informed

15.1 The Organisation shall provide the information set out in Part 15.2 to every data subject:

a) where personal information is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

b) where personal information is obtained from a third party, the relevant data subjects will be informed of its purpose:

i) if the personal information is used to communicate with the data subject, when the first communication is made; or

ii) if the personal information is to be transferred to another party, before that transfer is made; or

iii) as soon as reasonably possible and preferably not more than one month after the personal information is obtained.

15.2 The following information shall be provided in the form of a privacy notice:

a) details of the Organisation including, but not limited to, contact details, and the names and contact details of any applicable representatives and its Information Officer;

b) the purpose(s) for which the personal information is being collected and will be processed (as detailed in Part 23 of this Policy);

c) where applicable, the legitimate interests upon which the Organisation is justifying its collection and processing of the personal information;

d) where the personal information is to be transferred to a third party that is located outside of South Africa, details of that transfer, including but not limited to the safeguards in place (see Part 30 of this Policy for further details);

e) details of the data subject's rights under POPIA;

f) details of the data subject's right to withdraw their consent to the Organisation's processing of their personal information at any time;

g) details of the data subject's right to complain to the Information Regulator's;

h) details of any automated decision-making or profiling that will take place using the personal information, including information on how decisions will be made, the significance of those decisions, and any consequences.

16. Data Subject Access

16.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal information which the Organisation holds about them, what it is doing with that personal information, and why.

16.2 Data subjects wishing to make a SAR should do using a Subject Access Request Form 1, sending the form to the Organisation's Information Officer

16.3 Responses to SARs must normally be made within one month of receipt, however, this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

16.4 All SARs received shall be handled by the Organisation's Information Officer and in accordance with the Organisation's Data Subject Access Request Policy & Procedure.

16.5 The Organisation may charge a reasonable fee for the handling of normal SARs. The Organisation reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

17. Rectification of Personal information

17.1 Data subjects have the right to require the Organisation to rectify any of their personal information that is inaccurate or incomplete.

17.2 The Organisation shall rectify the personal information in question, and inform the data subject of that rectification, within one month of the data subject informing the Organisation of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

17.3 The Organisation may decline a data subject's request for personal information to be corrected and will keep a record of such request and the basis for declining the application.

18. Erasure of Personal information

18.1 Data subjects have the right to request that the Organisation erases the personal information it holds about them in the following circumstances:

a) it is no longer necessary for the Organisation to hold that personal information with respect to the purpose(s) for which it was originally collected or processed;

b) the data subject wishes to withdraw their consent to the Organisation holding and processing their personal information;

c) the data subject objects to the Organisation holding and processing their personal information (and there is no overriding legitimate interest to allow the Organisation to continue doing so) (see Part 20 of this Policy for further details concerning the right to object);

d) the personal information has been processed unlawfully;

e) the personal information needs to be erased in order for the Organisation to comply with a particular legal obligation.

18.2 Unless the Organisation has reasonable grounds to refuse to erase personal information, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

19. Restriction of Personal information Processing

19.1 Data subjects may request that the Organisation ceases processing the personal information it holds about them. If a data subject makes such a request, the Organisation shall retain only the amount of personal information concerning that data subject (if any) that is necessary to ensure that the personal information in question is not processed further.

20. Objections to Personal information Processing

20.1 Data subjects have the right to object to the Organisation processing their personal information based on legitimate interests or for direct marketing.

20.2 Where a data subject objects to the Organisation processing their personal information based on its legitimate interests, the Organisation shall cease such processing immediately, unless it can be demonstrated that the Organisation's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

20.3 Where a data subject objects to the Organisation processing their personal information for direct marketing purposes, the Organisation shall cease such processing promptly.

21. Direct Marketing

21.1 The Organisation is subject to certain rules and regulations when marketing its products and/or services.

21.2 The prior consent of data subjects is required for electronic direct marketing including email, text messaging, and automated telephone calls subject to the following limited exception:

a) The Organisation may send marketing text messages or emails to a customer provided that that customer's contact details have been obtained in the course of a sale, the marketing relates to similar products or services, and the customer in question has given permission to the Organisation to do so. Further to this, the customer is given the opportunity to opt-out of marketing in every subsequent communication from the Organisation.

21.3 Direct marketing to data subjects, except as provided for in Part 22.2(a) above, may only take place upon being presented with written consent from the data subject. The Direct Marketing Consent Form is to be used for this purpose.

21.4 The right to object to direct marketing shall be explicitly offered to data subjects in a clear and intelligible manner and must be kept separate from other information in order to preserve its clarity.

21.5 If a data subject objects to direct marketing, their request must be complied with promptly. A limited amount of personal information may be retained in such circumstances to the extent required to ensure that the data subject's marketing preferences continue to be complied with.

22. Personal information Collected, Held, and Processed

The following personal information is collected, held, and processed by the Organisation (for details of data retention, please refer to the Organisation's Personal Information Retention Policy):

Information	How We Collect the Personal Information
Identity Information including but not limited to identity numbers, drivers licences, passport numbers, names, surnames, Organisation / entity names and registration details, CCTV footage.	As far as practicably possible directly from the data subject. If not practicable possible to obtain such information directly from you, we will obtain such personal information from third parties.
Contact and location information including but not limited to telephone, email addresses, physical addresses, postal addresses, geographical location data.	As far as practicably possible directly from the data subject. If not practicable possible to obtain such information directly from you, we will obtain such personal information from third parties.
Business information including but not limited to ownership, shareholding, job titles, professions, email communication of an implicit or explicit private and confidential nature, affiliations, products, services, statutory registration information.	As far as practicably possible directly from the data subject. If not practicable possible to obtain such information directly from you, we will obtain such personal information from third parties or public forums where you may have made your personal information deliberately public.
Payment information including but not limited to transaction history, bank statements, invoices, credit notes, credit / debit card details, bank account numbers.	As far as practicably possible directly from the data subject. If not practicable possible to obtain such information directly from you, we will obtain such personal information from third parties.
Data from third parties including the verification of information.	As far as practicably possible directly from the data subject. If not practicable possible to obtain such information directly from you, we will obtain such personal information from third parties.

23. **Data Security - Transferring Personal information and Communications**

The Organisation shall ensure that the following measures are taken with respect to all communications and other transfers involving personal information:

23.1 All emails containing personal information must be encrypted;

23.2 All emails containing personal information must be marked “confidential”;

23.3 Personal information may be transmitted over a public wireless network due to the nature of our operations;

23.4 Personal information contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted by i.e., emptying the “Trash”

or “Deleted Items” folders associated with an email address.

23.5 Where personal information is to be transferred in hardcopy form it should be passed directly to the recipient or sent using the organisation’s courier services.

23.6 All personal information to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked “confidential”;

24. Data Security - Storage

The Organisation shall ensure that the following measures are taken with respect to the storage of personal information:

24.1 All electronic copies of personal information should be stored securely using passwords and built in data encryption;

24.2 All hardcopies of personal information, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;

24.3 All personal information stored electronically should be backed up to the cloud and will be encrypted and password protected.

24.4 No personal information should be transferred to any device personally belonging to an employee, agent, contractor, or other party working on behalf of the Organisation and personal information may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Organisation where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Protection of Personal Information Act (which may include demonstrating to the Organisation that all suitable technical and organisational measures have been taken);

25. Data Security - Disposal

When any personal information is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and/or disposed of. For further information on the deletion and disposal of personal information, please refer to the Organisation’s Personal Information Retention Policy.

26. Data Security - Use of Personal information

The Organisation shall ensure that the following measures are taken with respect to the use of personal information:

26.1 No personal information may be shared informally and if an employee, agent, contractor, or other party working on behalf of the Organisation requires access to any personal information that they do not already have access to, such access should be formally requested from the Deputy Information Officer

26.2 No personal information may be transferred to any employee, agent, contractor, or other party, whether such parties are working on behalf of the Organisation or not, without the authorisation of the Deputy Information Officer

26.3 Personal information must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, contractors, or other parties at any time;

26.4 If personal information is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;

26.5 Where personal information held by the Organisation is used for marketing purposes, it shall be the responsibility of the Chief Communications and Content Officer to ensure that the appropriate consent is obtained and that no data subjects have opted out;

27. Data Security - IT Security

The Organisation shall ensure that the following measures are taken with respect to IT and information security:

27.1 All passwords used to protect personal information should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols;

27.2 Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Organisation, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT service providers do not have access to passwords;

27.3 All software (including, but not limited to, applications and operating systems) shall be kept up to date. The Organisation's IT service provider shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so;

27.4 No software may be installed on any Organisation-owned computer or device without the prior approval of the Support Services Manager.

28. Organisational Measures

The Organisation shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal information:

28.1 All employees, agents, contractors, or other parties working on behalf of the Organisation shall be made fully aware of both their individual responsibilities and the Organisation's responsibilities under the Protection of Personal Information Act and this Policy, and shall be provided with a copy of this Policy;

28.2 Only employees, agents, contractors, or other parties working on behalf of the Organisation that need access to, and use of, personal information in order to carry out their assigned duties correctly shall have access to personal information held by the Organisation;

28.3 All sharing of personal information shall comply with the information provided to the relevant data subjects and, if required, the consent of such data subjects shall be obtained prior to the sharing of their personal information;

28.4 All employees, agents, contractors, or other parties working on behalf of the Organisation handling personal information will be appropriately supervised;

28.5 All employees, agents, contractors, or other parties working on behalf of the Organisation handling personal information shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal information, whether in the workplace or otherwise;

28.6 Methods of collecting, holding, and processing personal information shall be regularly evaluated and reviewed;

28.7 All personal information held by the Organisation shall be reviewed periodically, as set out in the Organisation's Personal Information Retention Policy;

28.8 The performance of those employees, agents, contractors, or other parties working on behalf of the Organisation handling personal information shall be regularly evaluated and reviewed;

28.9 All employees, agents, contractors, or other parties working on behalf of the Organisation handling personal information will be bound to do so in accordance with the principles of POPIA and this Policy by contract;

28.10 All agents, contractors, or other parties working on behalf of the Organisation handling personal information must ensure that any and all of their employees who are involved in the processing of personal information are held to the same conditions as those relevant employees of the Organisation arising out of this Policy and POPIA;

28.11 Where any agent, contractor or other party working on behalf of the Organisation handling personal information fails in their obligations under this Policy that party shall indemnify and hold harmless the Organisation against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure;

29. Transferring Personal information to a Country Outside South Africa

29.1 The Organisation may, from time to time, transfer ('transfer' includes making available remotely) personal information to countries outside of South Africa. POPIA restricts such transfers to ensure that the level of protection given to data subjects is not compromised.

29.2 Personal information may only be transferred to a country outside the South Africa if one of the following applies:

a) The personal information transferred to another country is protected by appropriate legislation; or

b) adequate safeguards are in place including binding corporate rules; or

c) a binding agreement is concluded between the Organisation and a third party that offers adequate protection; or

d) the transfer is made with the informed and explicit consent of the relevant data subject(s); or

e) The transfer is necessary for the performance of a contract between the data subject and the Organisation; or

f) for the establishment, exercise, or defence of legal claims; or

g) for the benefit of the data subject where it not reasonably practicable to obtain consent from the data subject and the data subject would most likely not have objected;

h) or the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party.

29.3 The Organisation may transfer personal information to Countries where the Organisation's data is stored by Microsoft, Pastel, Salesforce and Azzure and in accordance with an agreement that offers an adequate level of protection.

30. Data Breach Notification

30.1 All personal information breaches must be reported immediately to the Organisation's Information Officer.

30.2 If an employee, agent, contractor, or other party working on behalf of the Organisation becomes aware of or suspects that a personal information breach has occurred, they must not attempt to investigate it themselves. Any and all evidence relating to the personal information breach in question should be carefully retained.

30.3 If a personal information breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Information Officer must ensure that the Information Regulator's Office as well as the data subject(s) are in writing informed of the breach without delay after having become aware of it, unless such disclosure will interfere with a criminal investigation.

30.4 Data breach notifications shall include the following information:

a) The categories and approximate number of data subjects concerned;

b) The categories and approximate number of personal information records concerned;

c) The name and contact details of the Organisation's Information Officer (or other contact point where more information can be obtained);

d) The likely consequences of the breach;

e) Details of the measures taken, or proposed to be taken, by the Organisation to address the breach including, where appropriate, measures to mitigate its possible adverse effects and to prevent it from reoccurring.

31. Employee Personal Information

The Organisation holds a range of personal information about its employees. Employee personal information shall be collected, held, and processed in accordance with employee data subjects' rights and the Organisation's obligations under the Protection of Personal Information Act and with this Policy. The Organisation may collect, hold, and process the employee personal information detailed in this Policy, but not limited to:

31.1 Identification and other information relating to employees:

a) Name and surname;

b) Contact Details;

c) Addresses;

d) Identification documentation;

e) Work permits;

f) Bank details;

g) Tax number;

h) Next of kin information;

i) Vehicle details (if applicable);

j) Biometrics;

k) Qualifications;

31.2 Employment Equity monitoring information (Please refer to Part 33, below, for further information):

a) Age;

b) Gender;

c) Ethnicity;

d) Nationality;

e) Culture;

31.3 Health records (Please refer to Part 34, below, for further information):

a) Details of sick leave;

b) Medical conditions;

c) Disabilities;

d) Medical fitness reports;

31.4 Employment records:

a) Interview notes;

b) CVs, application forms, covering letters, reference checks and similar documents;

c) Assessments, performance reviews, and similar documents;

d) Details of remuneration including salaries, pay increases, bonuses, commission, overtime, benefits, and expenses;

e) Details of trade union membership where applicable. Please refer to Part 36, below, for further information);

f) Employee monitoring information (please refer to Part 37, below, for further information);

g) Records of disciplinary matters including reports and warnings, both formal and informal;

h) Details of grievances including documentary evidence, notes from interviews, procedures followed, and outcomes;

32. Employment Equity and Broad Based Black Economic Empowerment Information

32.1 The Organisation collects, holds, and processes certain information for the purposes of Employment Equity and Broad Based Black Economic Empowerment. Some of the personal information collected for this purpose, such as details of race, gender and disabilities falls within POPIA's definition of special personal information (see Part 2 of this Policy for a definition). Where possible, such special personal information will be de-identified. Where special personal information remains, it will be collected, held, and processed strictly in accordance with the conditions for processing special personal information, as set out in Part 6.2 of this Policy. The Organisation's lawful basis for processing such data is found in the Employment Equity Act, the Broad Based Black Economic Empowerment Act and relevant regulations.

32.2 Non-anonymised special personal information under this part, shall be accessible and used only by senior management and shall not be revealed to other employees, agents, contractors, or other parties working on behalf of the Organisation, except in exceptional circumstances where it is necessary to protect the legitimate interests of

the employee data subject(s) concerned, and such circumstances satisfy one or more of the conditions set out in Part 6.2 of this Policy.

33. Employee Health Records

33.1 The Organisation holds health records on employee data subjects which are used to assess the health, wellbeing, and welfare of employees and to highlight any issues which may require further investigation. In particular, the Organisation places a high priority on maintaining health and safety in the workplace and on preventing discrimination on the grounds of disability or other medical conditions. In most cases, health information on employees falls within POPIA's definition of special personal information (see Part 2 of this Policy for a definition). Any and all data relating to employee data subjects' health, therefore, will be collected, held, and processed strictly in accordance with the conditions for processing special category personal information, as set out in Part 6.2 of this Policy. The Organisation's lawful basis for processing employees' health information is as provided for in relevant labour related legislation such as The Basic Conditions of Employment Act, The Mines Health and Safety Act, The Occupational Health and Safety Act, the Labour Relations Act and the National Road Traffic Act.

33.2 Health records shall be accessible and used only by the HR Specialist and Exco and shall not be revealed to other employees, agents, contractors, or other parties working on behalf of the Organisation without the express consent of the employee data subject(s) to whom such data relates, except in exceptional circumstances where it is necessary to protect the legitimate interests of the employee data subject(s) concerned, and such circumstances satisfy one or more of the conditions set out in Part 6.2 of this Policy.

33.3 Health records will only be collected, held, and processed to the extent required to justify an employee's absence from work on account of illness and to ensure that employees are able to perform their work correctly, legally, safely, and without unlawful or unfair impediments or discrimination.

34. Employee Benefits

34.1 In cases where employee data subjects are enrolled in benefit schemes which are provided by the Organisation, it may be necessary from time to time for third party organisations to collect personal information from relevant employee data subjects.

34.2 Prior to the collection of such information, employee data subjects will be fully informed of the personal information that is to be collected, the reasons for its collection, and the manner in which it will be processed, as per the information requirements set out in Part 15 of this Policy.

34.3 The Organisation shall not use any such personal information except insofar as is necessary in the administration of the relevant benefits schemes.

34.4 The following schemes are available to employees. Please note that not all schemes may be applicable to all employees:

Old Mutual Pension SuperFund. For further information, please contact HR and/or Old Mutual. The following personal information may be collected, held, and processed:

a) Name and surname;

b) Contact Details;

c) Addresses;

d) Identification documentation;

e) Work permits;

f) Bank details;

g) Tax number;

h) Pension beneficiaries

35. Employee Monitoring

35.1 The Organisation may from time to time monitor the activities of employee data subjects. Such monitoring may include, but will not necessarily be limited to, internet, email and telephonic communication monitoring, vehicle and electronic communication devices' location tracking, CCTV monitoring of Organisation property, including drivers operating Organisation vehicles and access control to the workplace and/or for the use of Organisation equipment. In the event that monitoring of any kind is to take place (unless exceptional circumstances, such as the investigation of criminal activity or a matter of equal severity, justify covert monitoring), employee data subjects will be informed of the exact nature of the monitoring in advance.

35.2 Monitoring should not (unless exceptional circumstances justify it, as above) interfere with an employee's normal duties.

35.3 Monitoring will only take place if the Organisation considers that it is necessary to achieve the benefit it is intended to achieve. Personal information collected during any such monitoring will only be collected, held, and processed for reasons directly related to (and necessary for) achieving the intended result and, at all times, in accordance with employee data subjects' rights and the Organisation's obligations under the Protection of Personal Information Act.

35.4 The Organisation shall ensure that there is no unnecessary intrusion upon employee data subjects' personal communications or activities, and under no circumstances will monitoring take place outside of an employee data subject's normal place of work or work hours, unless the employee data subject in question is using any Organisation equipment or other facilities including, but not limited to, Organisation email, Office 365 platforms, intranet, work related Whatsapp groups or a virtual private network ("VPN") service provided by the Organisation for employee use, Organisation vehicles or electronic communication, storage and

computing devices.

36. Sharing Personal Information of Employee Data Subjects

36.1 The Organisation will endeavour to only share employee personal information with third parties that have specific safeguards in place such a POPIA compliance policies.

36.2 Employee personal information may be shared with clients of the Organisation, other employees, agents, contractors, or other parties working on behalf of the Organisation if the recipient has a legitimate, job-related need-to-know. If any employee personal information is to be shared with a third party located outside of South Africa, the provisions of Part 29, above, shall also apply.

36.3 Where a third-party Operator is used, that Operator shall process personal information on behalf of the Organisation only on the written agreement of the Organisation an in accordance with the guidelines and security measures agreed to.

37. Implementation of Policy

This Policy shall be deemed effective as of 1 July 2021. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

38. Disciplinary Measures

Contravention of this policy, whether intentionally or not, may result in disciplinary action taken. Such disciplinary action may include corrective measures but does not exclude the possibility of termination of employment under certain circumstances.

This Policy has been approved and authorised by:

Name:	Yandiswa Xhakaza
Position:	CEO
Date:	16 September 2021
Due for Review by:	31 August 2022
Signature: