COMPANY NAME: TA Matters

PROTECTION OF PERSONAL INFORMATION (POPI) POLICY

Implementation date	August 2023
Policy Owner	Karen Pratt

1. INTRODUCTION

1.1. This policy forms part of TA Matters's (hereinafter referred to as the company) policies and procedures.

1.2. The right to privacy is an integral human right recognised and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 ("POPIA")

1.3. "POPIA" aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information.

1.4. " POPIA" aims to balance the competing interests of:

- Our individual constitutional rights to privacy (which requires our personal information to be protected); and
- The needs of our society to have access to and to process (work with) our personal information for legitimate purposes, including the purpose of doing business.

1.5. Through the provision of Learning & Development Services (including training, coaching, facilitation and supervision), the company is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of customers, suppliers, employees, and other stakeholders.

1.6. A person's right to privacy entails having control over his or her personal information and being able to conduct his or her affairs relatively free from unwanted intrusions.

1.7. Given the importance of privacy, the company is committed to effectively managing personal information in accordance with POPIA's provisions and acknowledge we are accountable for looking after such information.

2. DEFINITIONS

Biometrics

Means a technique of personal identification that is based on physical, physiological, or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning, and voice recognition.

Child

Means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning them.

Competent Person

Means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.

Consent

Means any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of personal information.

Constitution

Means the Constitution of the Republic of South Africa, 1996.

Data Subject

This refers to the natural or juristic person to whom personal information relates such as an individual client, customer or a company that supplies the company with products or other goods.

De-Identify

In relation to personal information of a data subject, this means to delete any information that:

- identifies the data subject;
- can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
- can be linked by a reasonably foreseeable method to other information that identifies the data subject, and ''de-identified'' has a corresponding meaning;

Direct Marketing

Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:

- Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or
- Requesting the data subject to make a donation of any kind for any reason.

Operator

Means a person who processes personal information on behalf of the responsible party.

Personal information

This means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

- 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;
- Information relating to the education or the medical, financial, criminal or employment history of the person;
- Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier, or other particular assignment to the person;
- The biometric information of the person;
- The personal opinions, views, or preferences of the person;
- 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;
- The views or opinions of another individual about 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.

Processing

Where reference is made to the "processing" of personal information, this will include any activity in which the information is worked with, from the time that the information is collected, up to the time that the information is destroyed, regardless of whether the information is worked with manually, or by automated systems.

Public Record

Means a record that is accessible in the public domain, and which is in the possession of or under the control of a public body, whether or not it was created by that public body.

Record

Means any recorded information, regardless of form or medium, including:

- Writing on any material;
- 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;
- Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
- Book, map, plan, graph, or drawing;
- 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.

Re-Identify

In relation to personal information of a data subject, this means to resurrect any information that has been de-identified, that:

- identifies the data subject;
- can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
- can be linked by a reasonably foreseeable method to other information that identifies the data subject and ''re-identified'' has a corresponding meaning.

Responsible party

The responsible party is the entity that needs the personal information for a particular reason and determines the purpose of and means for processing the personal information. In this case, the company is the responsible party.

The Information officer

The information officer is responsible for ensuring the company's compliance with POPIA.

Where no information officer is appointed, the head of the company will be responsible for performing the information officer's duties.

Once appointed, the information officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. Deputy information officers can also be appointed to assist the information officer.

Unique Identifier

Means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

3. PURPOSE

3.1. The purpose of this policy is to protect the company from the compliance risks associated with the protection of personal information which includes:

- Breaches of confidentiality;
- Failing to offer choice in that all data subjects should be free to choose how and for what purpose the company uses the information; and
- Reputational damage.

3.2. This policy demonstrates the company's commitment to protecting the privacy rights of data subjects in the following manner:

- Through stating desired behaviour and directing compliance with the provisions of POPIA and best practice;
- By cultivating a culture that recognises privacy as a valuable human right;
- By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information;
- By creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of the organisation;
- By assigning specific duties and responsibilities, including the appointment of an information officer and where necessary, deputy information officers in order to protect the interests of the organisation and data subjects; and
- By raising awareness through training.

4. APPLICATION

4.1. This policy and it guiding principles apply to:

- All shareholders of the company
- All business units and divisions of the company
- All employees
- All contractors, suppliers and other persons acting on behalf of the company.

5. THE COMPANY'S UNDERTAKING TO DATA SUBJECTS

5.1. The company undertakes:

- To follow POPIA at all relevant times and to process personal information lawfully and reasonably, so as not to infringe unnecessarily on the privacy of our data subjects;
- To process information only for the purpose for which it is intended, to enable the company to operate, as agreed with data subjects;
- To whenever necessary, obtain consent to process personal information;
- Where consent is not required, to follow legal obligations placed upon on the company in the processing of personal information, or to protect a legitimate interest that requires protection;
- To stop processing personal information if the required consent is withdrawn, or if a legitimate objection is raised;
- To collect personal information directly from the data subject, unless:
  - the information is of public record; or
  - the data subject has consented to the collection of their personal information from another source; or
  - the collection of the information from another source does not prejudice the data subject; or
  - the information to be collected is necessary for the maintenance of law and order or national security; or
  - the information is being collected to comply with a legal obligation, including an obligation to SARS; or
  - the information collected is required for the conduct of proceedings in any court or tribunal; where these proceedings have commenced or are reasonably contemplated; or
  - the information is required to maintain our legitimate interests; or
  - where requesting consent would prejudice the purpose of the collection of the information; or
  - where requesting consent is not reasonably practical in the circumstances.
- To retain records of the personal information collected for the minimum period as required by law unless the data subject has furnished their consent or instructed the company to retain the records for a longer period;
- To advise data subjects of the purpose of the collection of the personal information;
- To destroy or delete records of the personal information (so as to de-identify the data subject) as soon as reasonably possible after the time period for which we were entitled to hold the records have expired;
- To restrict the processing of personal information:
  - where the accuracy of the information is contested, for a period sufficient to enable the company to verify the accuracy of the information;
  - where the purpose for which the personal information was collected has been achieved and where the personal information is being retained only for the purposes of proof;

- where the data subject requests that the personal information is not destroyed or deleted, but rather retained; or
- where the data subject requests that the personal information be transmitted to another automated data processing system.

- The further processing of personal information shall only be undertaken:
  - where the further processing is compatible with the original purpose;
  - where the further processing is necessary because of a threat to public health or public safety or to the life or health of the data subject;
  - where the information is used for historical, statistical or research purposes and the identity of the data subject will not be disclosed; or
  - where this is required by the Information Regulator appointed in terms of POPI.
- To undertake to ensure that the personal information which the company collects, and processes is complete, accurate, not misleading and up to date;
- To undertake to retain the physical file and the electronic data related to the processing of the personal information;
- To undertake to take special care with data subject bank account details, and we are not entitled to obtain or disclose such banking details unless the data subjects' specific consent has been obtained.

6. DATA SUBJECTS RIGHTS

6.1. Where appropriate the company will ensure that its clients, customers, suppliers, and employees are made aware of the rights conferred upon them as data subjects.

6.2. The company will ensure it gives effect to the following rights:

6.2.1. The right to access personal information.

The company recognises that a data subject has the right:

- to establish what personal information the company holds about them and why;
- to access to their personal information; and
- to establish how to keep their personal information up to date.

On production of proof of identity, any person is entitled to request that the company confirms, free of charge, whether the company holds any personal information about themselves.

Access to information requests can be made by an email addressed to the information officer. The information officer will provide the data subject with a "Personal Information Request Form". Once the completed form is received the information officer will, on verification of identity, hand over the information. The information officer shall do this within a reasonable period of time, in a reasonable manner and in an understandable form.

In certain circumstances the company will be obliged to refuse to disclose the record containing the personal information to the data subject. In other circumstances the company will have discretion as to whether or not to do so. In all cases where the disclosure of a record will entail the

disclosure of information that is additional to the personal information of the person requesting the record, the written consent of the information officer (or the deputy) will be required, and that person shall make their decision having regard to the provisions of Chapter 4 part 3 of the Promotion of Access to Information Act If a request for personal information is made and part of the requested information may, or must be refused, every other part will still be disclosed.

6.2.2. The right to have personal information corrected or deleted.

A data subject is entitled to require the company to correct or delete personal information that the company has, which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or which has been obtained unlawfully.

A data subject is also entitled to require the company to destroy or delete records of personal information about the data subject that the company is no longer authorised to retain.

Any such request must be made on the" Request for correction or deletion of Personal Information Form".

Upon receipt of such a lawful request, the company will comply as soon as reasonably practicable.

In the event that a dispute arises regarding the data subject's rights to have information corrected, and in the event that the data subject so requires, the company will attach to the information, in a way that it will always be read with the information, an indication that the correction of the information has been requested but has not been made.

The company will notify the data subject who has made a request for their personal information to be corrected or deleted what action has been taken as a result of such a request.

6.2.3. **The right to object to the processing of personal information**

The data subject has the right, on reasonable grounds, to object to the processing of their personal information.

In such circumstances, the company will give due consideration to the request and the requirements of POPIA. The company may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the personal information.

6.2.4. **The right to object to direct marketing**

The data subject has the right to object to the processing of their personal information for purposes of direct marketing by means of unsolicited electronic communications.

6.2.5. **The right to complain to the information officer.**

The data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil

proceedings regarding the alleged non-compliance with the protection of their personal information. (Complaint Form")

6.2.6. **The right to be informed.**

The data subject has the right to be notified that their personal information is being collected by the company.

The data subject also has the right to be notified in any situation where the company has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

6.2.7. The right to withdraw consent.

In cases where the data subject's consent is required to process their personal information, this consent may be withdrawn.

7. GUIDING PRINCIPLES

The company will ensure that the below principles/conditions for lawful processing of personal information set out in POPIA, are complied with:

7.1. Condition 1 Accountability

The company must be accountable for the personal information it processes or holds in its possession.

7.2. Condition 2 - Processing Limitation

Personal information must be processed in a lawful and reasonable manner. The purpose for processing the information must be lawful, adequate, relevant, and not excessive.

7.3. Condition 3 - Purpose specification

The purpose for processing personal information must be specific, explicitly defined, and lawful.

7.4. Condition 4 - Further Processing Limitation

The reason for processing personal information further must be compatible with the original purpose of collection.

7.5. Condition 5 - Quality of Information

The company is required to take practicable steps to ensure that the personal information processed is complete, accurate, not misleading and updated.

7.6. Condition 6 - Openness

Personal information must be processed in a way that allows the data subject to know what is happening to their personal information.

7.7. Condition 7 - Security Safeguards

The company must ensure that there are sufficient security safeguards in place to secure the integrity and confidentiality of the personal information in our possession.

7.8. Condition 8 - Data subject participation

Data subjects have a right to access to their personal information and to correct and update their personal information.

8. SECURITY SAFEGAURDS

8.1. POPIA demands that company's take reasonable measures to protect personal information and to protect it at each step. In order to secure the integrity and confidentiality of the personal information in the company's possession and to protect it against loss or damage or unauthorised access, the company has implemented the following security safeguards:

- All personal data (structured and unstructured) in company processes (formal and informal) will be identified;
- A risk assessment of personal data will be completed;
- Company premises are protected by a burglar alarms and armed response;
- The company will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals. To this end, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification, or destruction;
- Paper records stored in a locked filing cabinet;
- All the user terminals on the company's internal computer network and servers are protected by passwords which must be changed on a regular basis;
- The company's website is hosted by Xneelo. Their data centre security is referenced here at https://xneelo.co.za/help-centre/products-and-services/security-and-reliability/
- The personal information of data subjects will be destroyed timeously in a manner that de-identifies the person;
- The processing of special personal information will be prohibited;
- Security safeguards will be verified on a regular basis to ensure that safeguards are continually updated and implemented in response to new risks or deficiencies.

- The company's operators and third-party service providers will be required to enter into service level agreements with the company where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.
- Regularly review contractual obligations of third parties; and
- The requirements of Information Officer and/or Information Regulator will be complied with.

9. SECURITY BREACHES

9.1. Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an unauthorised person, the company will report this to the Information Regulator and advise the relevant data subject/s, unless the company is no longer able to identify the data subject/s. This notification will take place as soon as reasonably possible.

9.2. Such notification will be given to the Information Regulator first as it is possible that they or another public body might require the notification to the data subject/s be delayed.

9.3. The notification to the data subject will be communicated in writing in one of the following ways, with a view to ensuring that the notification reaches the data subject:

- by mail to the data subject's last known physical or postal address;
- by email to the data subjects last known email address;
- by publication on the company's website or in the news media; or
- as directed by the information Regulator.

9.4. The notification to the data subject will give sufficient information to enable the data subject to protect themselves against the potential consequences of the security breach and must include:

- a description of the possible consequences of the breach;
- details of the measures that the company intends to take or have taken to address the breach;
- the recommendation of what the data subject could do to mitigate the adverse effects of the breach; and
- if known, the identity of the person who may have accessed, or acquired the personal information.

10. SPECIAL PERSONAL INFORMATION

10.1. Special rules apply to the collection and use of information relating to a person's religious or philosophical beliefs, their race or ethnic origin, their trade union membership, their political persuasion, their health or sex life, their biometric information, or their criminal behaviour.

10.2. The company shall not process any of this special personal information without the data subject's consent or where this is necessary for the establishment, exercise, or defence of a right or an obligation in law or the authorisation of the Regulator has been obtained.

10.3. In the normal course of business, it is unlikely that there will be a need to process special information, but should it be necessary the guidance of the information officer will be sought.

11. THE PROCESSING OF PERSONAL INFORMATION OF CHILDREN

11.1. The company will only process the personal information of a child if:

11.1.1. The prior consent of a competent person is obtained;

11.1.2. The information has been deliberately made public by the child with the consent of a competent person.

11.1.3. The processing is necessary:

11.1.3.1. for the establishment, exercise, or defence of aright or obligation in Law;

11.1.3.2. to comply an obligation of International Public law; or

11.1.3.3. for historical, statistical or research purposes

11.1.4. Application is made to the Regulator in the case of public interest.

12. DUTIES AND RESPONSIBILITIES

12.1. Information Officer

The company's information officer is Karen Pratt.

The information officer's responsibilities include:

- Ensuring compliance with POPIA;
- Dealing with requests which the company receives in terms of POPIA;
- Handling complaints;
- To facilitate cross-border co-operation; and
- Working with the Information Regulator in relation to investigations.

The information officer will designate, in writing, deputy information officers to perform the tasks mentioned above.

The information and deputy information officers will be registered with the Information Regulator prior to taking up their duties.

In carrying out their duties, the information officer will ensure that:

- This compliance policy is implemented, monitored, and maintained;
- A personal information Impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;
- Those internal measures are developed together with adequate systems to process requests for information or access to information;
- That internal awareness sessions are conducted regarding the provisions of POPIA; and
- That copies of th**e** policy are provided to persons at their request.

12.2. Employees and other Persons acting on behalf of the company.

- Employees and other persons acting on behalf of the company will during the course of the performance of their services, gain access to and become acquainted with the personal information of certain clients, suppliers, employees, and other parties and:
  - Are required to treat personal information as a confidential business asset and to respect

the privacy of data subjects;

- May not directly or indirectly, utilise, disclose, or make public in any manner to any person or third party, either within the company or externally, any personal information, unless such information is already publicly known, or the disclosure is necessary in order for the employee or person to perform his or her duties;
- Must request assistance from their line report or the information officer if they are unsure about any aspect related to the protection of a data subject's personal information;
- May only process personal information where:
  - the data subject, or a competent person where the data subject is a child, consents to the processing; or
  - the processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or
  - the processing complies with an obligation imposed by law on the company; or
  - the processing protects a legitimate interest of the data subject; or
  - the processing is necessary for pursuing the legitimate interests of the company or of a third party to whom the information is supplied.

- Personal information will only be processed where the data subject clearly understands why and for what purpose their personal information is being collected; and has granted the company with explicit written or verbally recorded consent to process their personal information.
- Employees and other persons acting on behalf of the company will consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.
- Consent to process a data subject's personal information will be obtained directly from the data subject, except where:
  - the personal information has been made public, or
  - where valid consent has been given to a third party, or
  - the information is necessary for effective law enforcement.

- Employees and other persons acting on behalf of the company will under no circumstances:
  - Process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties;
  - Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All personal information must be accessed and updated from the company's central database or a dedicated server;
  - Share personal information informally; or
  - Transfer personal information outside of South Africa without the express permission from the information officer.

- Employees and other persons acting on behalf of the company are responsible for:
  - Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy;
  - Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created;
  - Ensuring that personal information is encrypted prior to sending or sharing the information electronically;
  - Ensuring that all computers, laptops, and devices such as tablets, flash drives and smartphones that store personal information are protected by suitable and appropriate technological and best practice methodologies and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons;
  - Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks;
  - Ensuring that where personal information is stored on removable storage medias such as external drives, CDs, or DVDs that these are kept locked away securely when not being used;
  - Ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it and/or copy it;
  - Taking reasonable steps to ensure that personal information is kept accurate and up to date;
  - Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected; and
  - Undergoing POPIA awareness training from time to time.

- Where an employee, or a person acting on behalf of the company, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification on, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the information officer or the deputy information officer.

13. CIRCUMSTANCES REQUIRING PRIOR AUTHORISATION

13.1. The company will only process the personal information of a child with the consent of the child's parent or legal guardian.

13.2. Furthermore, In the following circumstances the company will require prior authorisation from the Information Regulator before processing any personal information:

- in the event that the company intends to utilise any unique identifiers of data subjects (account numbers, file numbers or other numbers or codes allocated to data subjects for the purposes of identifying them) for any purpose other than the original intention, or to link the information with information held by others;
- if the company is processing information on criminal behaviour, unlawful or objectionable conduct

or for the purposes of credit;

- if the company is transferring special personal information or the personal information of children to a third party in a foreign country, that does not provide adequate protection of that personal information.

13.3. The Information Regulator will be notified of the company's intention to process any personal information as set out above prior to any processing taking place and the company will not commence with such processing until the Information Regulator has decided in the company's favour. The Information Regulator has four (4) weeks to decide but may decide that a more detailed investigation is required. In this event the decision will be made in a period as indicated by the Information Regulator, which must not exceed thirteen (13) weeks. If the Information Regulator does not decide within the stipulated time periods, the company will assume that the decision is in the company's favour and commence processing the information.

14. TRANSBORDER INFORMATION FLOWS

14.1. The company will not transfer a data subject's personal information to a third party in a foreign country, unless:

- the data subject consents to this, or requests it; or
- such third party is subject to a law, binding corporate rules or a binding agreement which protects the personal information in a manner similar to POPIA, and such third party is governed by similar rules which prohibit the onward transfer of the personal information to a third party in another country; or
- the transfer of the personal information is required for the performance of the contract between the company and the data subject; or
- the transfer is necessary for the conclusion or performance of a contract for the benefit of the data subject entered into between the company and the third party; or
- the transfer of the personal information is for the benefit of the data subject, and it is not reasonably possible to obtain their consent and that if it were possible the data subject would be likely to give such consent.

15. DATA PROTECTION REGULATIONS

15.1. TA Matters shall comply with Data Protection Regulations implemented in other countries and/or regions and shall comply with any provisions as applicable to South Africa and/or cross border relationships/transactions between TA Maters and individuals (Personal or juristic) in such countries.

16. POPIA AUDIT

16.1. The company's information officer will schedule periodic POPIA Audits. The purpose of a POPIA audit is to:

- Identify the processes used to collect, record, store, disseminate and destroy personal information;

- Determine the flow of personal information throughout the company;
- Redefine the purpose for gathering and processing personal information;
- Ensure that the processing parameters are still adequately limited;
- Ensure that new data subjects are made aware of the processing of their personal information;
- Re-establish the rationale for any further processing where information is received via a third party;
- Verify the quality and security of personal information;
- Monitor the extent of compliance with POPIA and this policy; and
- Monitor the effectiveness of internal controls established to manage the company's POPIA related compliance risk.

16.2. In performing the POPIA audits, the information officer will liaise with management in order to identify areas within the company that are most vulnerable or susceptible to the unlawful processing of personal information.

17. POPIA COMPLAINT'S PROCEDURE

17.1. Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. The company will take all complaints very seriously and will address all POPIA related complaints in accordance with the following procedure:

- POPIA complaints must be submitted to the company in writing. Where so required, the information officer will provide the data subject with a "Complaint Form".
- Where the complaint has been received by any person other than the information officer, that person will ensure that the full details of the complaint reach the information officer within two (2) working days.
- The information officer will provide the complainant with a written acknowledgement of receipt of the complaint within two (2) working days.
- The information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the information officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA.
- The information officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on the company's data subjects.
- Where the information officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised person, the information officer will consult with the CEO/managing director whereafter the affected data subjects, and the Information Regulator will be informed of this breach.

- The information officer will revert to the complainant with a proposed solution with the option of escalating the complaint to the company's board within seven (7) working days of receipt of the complaint. In all instances, the company will provide reasons for any decisions taken and

communicate any anticipated deviation from the specified timelines.

- The information officer's response to the data subject must comprise any of the following:
  - A suggested remedy for the complaint,
  - A dismissal of the complaint and the reasons as to why it was dismissed, or
  - An apology (if applicable) and any disciplinary action that has been taken against any employees involved.
- Where the data subject is not satisfied with the information officer's suggested remedies, the data subject has the right to complain to the Information Regulator.
- The information officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPIA related complaints.
- Where a POPIA complaint or a POPIA infringement investigation has been finalised, the company may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy.

18. OFFENCES AND PENALTIES

18.1. POPIA provides for serious penalties for the contravention of its terms. Breaches of this compliance manual/policy will also be viewed as a serious disciplinary offence. It is therefore imperative that all employees comply strictly with the terms of this compliance manual/policy.

19. SCHEDULE OF ANNEXURES AND FORMS

Annexure A – Objection to the Processing of Personal Information Form

Annexure B - Request for the correction or deletion of Personal information Form

Annexure C - Personal Information Request Form

Annexure D - Complaint Form

Annexure E - Application for consent to direct marketing

Annexure F – Notice and Request for correction or deletion of personal information.

20. POLICY ADOPTION

Managing Director	
Name	Karen Pratt
Position	Managing Director
Signature	
Date	
Information Officer	
Name	Karen Pratt

Position	Managing Director
Signature	
Date	