| DOCUMENT NAME: POPI POLICY | |
|---|---|
| DOCUMENT TYPE: POPI COMPLIANCE | |
| | |

**PROTECTION OF PERSONAL INFORMATION POLICY**

Contents

## 1. INTRODUCTION

- 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 ("POPI").
- The POPI Act aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner.
- Through the provision of quality goods and services, the organisation is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, customers, employees and other stakeholders.
- 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.
- Given the importance of privacy, the company is committed to effectively managing personal information in accordance with the provisions as set out in the POPI Act.

## 2. DEFINITIONS

### 2.1 Personal Information

Personal information is any information that can be used to reveal a person's identity. Personal information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person (such as a company), including, but not limited to information concerning:

- race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a 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.
- 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.

**2.2 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 organisation with products or other goods.

**2.3 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, **Riversmead Poultry Farm** is the responsible party.

**2.4 Operator**

An operator means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. It is considered good practice for a responsible party to include a confidentiality clause, should the organisation make use of a third-party operator.

**2.5 Information Officer**

- The Information Officer is responsible for ensuring the organisation’s compliance with the POPI Act.

- Once appointed, the Information Officer must be registered with the South African Information Regulator established under the POPI Act prior to performing any duties.
- A Deputy Information Officer must also be appointed in line with the requirements of the Act where applicable based on the size of the organisation.

**2.6 Processing**

Processing of information includes any activity or any set of activities, whether or not by automatic means, concerning personal information and includes:

- the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use.
- dissemination by means of transmission, distribution or making available in any other form; or
- merging, linking, as well as any restriction, degradation, erasure or destruction of personal information.

**2.7 Record**

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

- Writing on any material.
- Information produced, recorded or stored by means of any type of 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.

**2.8 Filing System**

Means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

**2.9 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. (Employee number, Customer Reference number, ID number etc.)

**2.10 De-Identify.**

This means to delete any information that identifies a data subject, or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the data subject.

**2.11 Re-Identify.**

In relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

**2.12 Consent**

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

**2.13 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.

**2.14 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.

**2.15 Code of Conduct**

Means a code of conduct issued in terms of Chapter 7 of the Act.

**2.16 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.

**2.17 Child**

A child is 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 him- or herself.

---

**3. POLICY PURPOSE**

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. For instance, the company could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.
- Failing to offer choice. For instance, all data subjects should be free to choose how and for what purpose the company uses information relating to them.
- Reputational damage. For instance, the company could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by the company.

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 the POPI Act and best practice.
- By cultivating an organisational 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 to control owners, including the appointment of an Information Officer and where necessary, Deputy Information Officers to protect the interests of the company and data subjects.
- By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

**4. POLICY APPLICATION**

This policy and its guiding principles apply to:

- The organisation's governing body
- All branches, business units and divisions of the organisation
- All employees, workers and volunteers
- All contractors, suppliers and other persons acting on behalf of the organisation.

The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as the organisation's PAIA Policy as required by the Promotion of Access to Information Act (Act No 2 of 2000).

The legal duty to comply with the provisions of the POPI Act is activated in any situation where there is:

- **Processing** of **personal information** entered into a **record** by or for a **responsible person** who is **situated** in South Africa.

The POPI Act does not apply in situations where the processing of personal information:

- is concluded in the course of purely personal or household activities, or
- where the personal information has been de-identified.

**5. RIGHTS OF DATA SUBJECTS**

Everyone has the right to be informed if someone is collecting their personal information, or if their personal information has been accessed by an unauthorised person. In addition, they have the right of access to their personal information and to acquire that personal information to be corrected or destroyed, or they may object to their personal information being processed.

**5.1 The POPI Act does not apply to personal information processed.**

- In the course of a personal or household activity
- Where the processing authority is a public body involved in National Security, Defense, Public Safety, or money laundering.

- The Cabinet or Executive Council of the Province
- As part of a judicial function.

**5.2 Personal Information can only be processed.**

- With the consent of the data subject
- If it is necessary for the conclusion or performance of a contract to which the data subject is a party,
- If it is required by law
- If it protects a legitimate interest of the data subject
- If it is necessary to pursue your legitimate interests or the interest of a third party to whom the information is supplied.

Everyone has the right to object to having the personal information processed. They have the right to withdraw their consent or object if they can show legitimate grounds for their objection.

**5.3 A responsible party has to collect personal information directly from the data subject, unless**

- The information is contained in some public record or has been deliberately published by the data subject.
- Collecting information from another source does not prejudice the data subject.
- It is necessary for some public purpose or to protect their own interests.
- Obtaining the information directly from the subject would prejudice a lawful purpose or is not reasonably possible.

Personal information may only be collected for a specific, explicitly defined and lawful purpose and the data subject must be aware of the purpose for which the information is being

collected.

Once personal information is no longer needed for the specific purpose for which it was gathered, it must be disposed of or the data must be “de-identified”.

Personal Information may only be kept if it is allowed by law, or the information is needed to keep record for lawful purpose or in accordance with the contract between the company and the data subject, or the data subject has consented to the data processor keeping the records.

The company is entitled to keep records of personal information for historical, statistical or research purposes, if it has been “de-identified” and safeguards have been established to prevent the records being used for any other purposes.

Records must be destroyed in a way that prevents them from being reconstructed.

Personal information may only be used for the purpose which the data was collected.

Documentation relating to personal information and how it has been processed must be maintained as referred to in section 14 or 51 of the Promotion of Access to Information Act.

**5.4 When information is being collected, data subjects must be made aware of**

- The information that is being collected and if the information is not being collected from the subject must be made aware of the source from which the information is being collected.
- The name and address of the person / organisation collecting the information.
- The purpose of collecting the information.
- What period the information will be retained for, and assurance given that it will be destroyed by the given date
- Whether the supply of the information by the subject is voluntary or mandatory.

- The consequences of failure to provide the information.
- Whether the information is being collected in accordance with any law.
- If it is intended for the information to leave the country and what level of protection will be afforded to the information after it has left South Africa.
- Who will be receiving the information?
- That the data subject has access to the information and the right to rectify any details
- The data subject has the right to object to the information being processed (if such right exists.)
- That the data subject has the right to lodge a complaint with the Information Regulator. (The contact details of the Information Regulator must also be supplied.)

**6. GENERAL GUIDING PRINCIPLES**

All employees and persons acting on behalf of Company will always be subject to, and act in accordance with, the following guiding principles:

**6.1 Accountability**

- Failing to comply with the POPI Act could potentially damage the company's reputation or expose the company to a civil claim for damages. (The protection of personal information is therefore everybody's responsibility.)
- The company will ensure that the provisions of the POPI Act and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour.
- The company will take appropriate steps, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.

**6.2 Processing Limitation**

The company will ensure that personal information under its control is processed:

- in a fair, lawful and non-excessive manner, and

- only with the informed consent of the data subject, and
- only for a specifically defined purpose.

- The company will inform the data subject of the reasons for collecting personal information and obtain written consent prior to processing such personal information.
- Alternatively, where services or transactions are concluded over the telephone or electronic video feed, the organisation will maintain a voice recording of the stated purpose for collecting the personal information followed by the data subject's subsequent consent.
- The company will under no circumstances distribute or share personal information between separate legal entities, associated organisations or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected.
- Where applicable, the data subject will be informed of the possibility that their personal information will be shared with other aspects of the organisation's business and be provided with the reasons for doing so.

**6.3 Purpose Specification**

- All the company's business units and operations must be informed by the principle of transparency.
- The company will process personal information only for specific, explicitly defined, and legitimate reasons.
- The company will inform data subjects of these reasons prior to collecting or recording the data subject's personal information.

**6.4 Further Processing Limitation**

- Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose.

- Therefore, where the company seeks to process personal information, it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, the company will first obtain additional consent from the data subject.

**6.5 Information Quality**

- The company will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading.
- The company will ensure that information accuracy is regarded as highly important.
- Where personal information is collected or received from third parties, the company will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the data subject or by way of independent sources.

**6.6 Open Communication**

- The company will take reasonable steps to ensure that data subjects are notified that their personal information is being collected including the purpose for which it is being collected and processed.
- The company will ensure that it will have procedures in place for data subjects who want to:
    - Enquire whether the company holds related personal information, or
    - Request access to related personal information, or
    - Request the company to update or correct related personal information, or
    - Make a complaint concerning the processing of personal information.

**6.7 Security Safeguards**

- The company will manage the security of its filing system to ensure that personal information is adequately protected.

- To this end, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction of personal information.
- Security measures will be context-sensitive protected manner.
- The company will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on the organisation's IT network.
- The company will ensure that all paper and electronic records with personal information are securely stored and made accessible only to authorised individuals.
- All new employees will be required to sign an employment contract containing contractual terms for the use and storage of their employee information.
- Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which the company is responsible.
- All existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment contracts containing the relevant consent and confidentiality clauses.
- 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 the POPI Act and the lawful processing of any personal information pursuant to the agreement.

**6.8 Data Subject Participation**

- A data subject may request the correction or deletion of their personal information held by the company.
- The company will ensure that it provides a facility for data subjects who want to request the correction or deletion of their personal information.
- Where applicable, the company will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

## 7. INFORMATION OFFICERS

- The Company will appoint an Information Officer and where necessary, a Deputy Information Officer to assist the Information Officer.
- The company's Information Officer is responsible for ensuring compliance with the POPI Act.
- Appointing an Information Officer is considered to be a good business practice.
- Consideration will be given on an annual basis to the re-appointment or replacement of the Information Officer and the reappointment or replacement of any Deputy Information Officers.
- Once appointed, the company will register the Information Officer with the South African Information Regulator established under the POPI Act prior to performing his or her duties.

## 8. SPECIFIC DUTIES AND RESPONSIBILITIES

### 8.1 Governing Body

The company's governing body cannot delegate its accountability and is ultimately answerable for ensuring that the company meets its legal obligations in terms of the POPI Act.

The company may however delegate some of its responsibilities in terms of the POPI Act to management or other capable individuals.

The governing body is responsible for ensuring that:

- The organisation appoints an Information Officer, and where necessary, a Deputy Information Officer.
- All persons responsible for the processing of personal information on behalf of the company:
    - are appropriately trained and supervised to do so,

    - understand that they are contractually obligated to protect the personal information they come into contact with, and
    - are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.
- Data subjects who want to make enquires about their personal information are made aware of the procedure that needs to be followed should they wish to do so.
- The scheduling of a periodic POPI Audit to accurately assess and review the ways in which the organisation collects, holds, uses, shares, discloses, destroys and processes personal information.

**8.2 Information Officer**

The organisation's Information Officer is responsible for:

- Take steps to ensure the organisation's reasonable compliance with the provision of the POPI Act.
- Responsible to inform and update the board of the organisation's responsibilities with regards to personal information protection as set out by the POPI Act.
- Analyse privacy regulations and align all Company Policies and Procedures
- Schedule and conduct compliance audits on a regular basis
- Ensure that the Company has due processes in place for data subjects who want to update their information or for submitting complaints.
- Review any contracts entered into with operators, employees, and other 3rd parties. Ensure said contracts are aligned evaluate the impact it may have on any personal information the organisation may have.
- Responsible to encourage compliance with the conditions for lawful processing of personal information.
- Ensure that employees and other persons acting on behalf of the Organisation are fully aware of the risks associated with the processing of personal information.

- Ensure that employees and other persons acting on behalf of the Organisation are updated about all security controls in place to protect personal information.
- Organise and oversee awareness training of all involved in processing of personal information on behalf of the Organisation.
- Address any queries or concerns from employees regarding the POPI Act and how it impacts them.
- Address any POPI related requests or complaints made by a data subject.
- Work with the Information Regulator in the event of any investigations. The Information Officer will therefore act as the contact point for the Information Regulator on issues relating to the processing of Personal Information and will consult with the Information Regulator where appropriate, with regards to any other matter.
- The Deputy information Officer will assist the Information officer with all duties stipulated above as and when required.

**8.3 IT Manager/ IT Service Provider**

The organisation's IT Manager/IT Service Provider is responsible for:

- Ensuring that the organisation's IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards.
- Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services.
- Ensuring that servers containing personal information are sited in a secure location, away from the general office space.
- Ensuring that all electronically stored personal information is backed-up and tested on a regular basis.
- Ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion, and malicious hacking attempts.
- Ensuring that personal information being transferred electronically is encrypted.

- Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software.
- Performing regular IT audits to ensure that the security of the organisation's hardware and software systems are functioning properly.
- Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons.
- Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on the organisation's behalf. For instance, cloud computing services.

**8.4 Employees and other Persons acting on behalf of the Organisation.**

Employees and other persons acting on behalf of the organisation will, during the course of the performance of their services, gain access to and become acquainted with the personal information of certain clients, suppliers, and other employees.

Employees and other persons acting on behalf of the organisation are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

Employees and other persons acting on behalf of the organisation may not directly or indirectly, utilise, disclose, or make public in any manner to any person or third party, either within the organisation 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.

Employees and other persons acting on behalf of the organisation must request assistance from their line manager or the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.

Employees and other persons acting on behalf of the organisation will 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 responsible party; or
- The processing protects a legitimate interest of the data subject; or
- The processing is necessary for pursuing the legitimate interests of the organisation or of a third party to whom the information is supplied.

*Furthermore, personal information will only be processed where the data subject:*

- Clearly understands why and for what purpose his, her or its personal information is being collected; and
- Has granted the organisation with explicit written or verbally recorded consent to process his, her or its personal information.

Employees and other persons acting on behalf of the organisation 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.

Informed consent is therefore when the data subject clearly understands for what purpose his, her or its personal information is needed and who it will be shared with.

Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, the

organisation will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.

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 organisation 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 organisation's central database or a dedicated server.
- Share personal information informally. Personal information should never be sent by email, as this form of communication is not secure. Where access to personal information is required, this may be requested from the relevant line manager or the Information Officer.
- Transfer personal information outside of South Africa without the express permission from the Information Officer.

*Employees and other persons acting on behalf of the organisation 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. The IT Manager/ Service Provider will assist employees and where required, other persons acting on behalf of the organisation, with the sending or sharing of personal information to or with authorised external persons.
- Ensuring that all computers, laptops, and devices such as tablets, flash drives and smartphones that store personal information are password protected 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. For instance, in a locked drawer of a filing cabinet.
- Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer.
- Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or customer phones or communicates via email. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the Information Officer to update the information accordingly.
- 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.

Where personal information is no longer required, authorisation must first be obtained from the relevant line manager or the Information Officer to delete or dispose of the personal information in the appropriate manner.

- Undergoing POPI Awareness training from time to time.

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

**9. POPI AUDIT**

The organisation's Information Officer will schedule periodic POPI Audits.

The purpose of a POPI audit is to:

- Identify the processes used to collect, record, store, disseminate and destroy personal information.
- Determine the flow of personal information throughout the organisation. For instance, the organisation's various business units, divisions, branches, and other associated organisations.
- 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 extend of compliance with POPIA and this policy.

- Monitor the effectiveness of internal controls established to manage the organisation's POPI related compliance risk.
- In performing the POPI Audit, Information Officer will liaise with line managers in order to identify areas within in the organisation's operation that are most vulnerable or susceptible to the unlawful processing of personal information.
- Information Officers will be permitted direct access to and have demonstrable support from line managers and the organisation's governing body in performing their duties.

**10. REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE**

Data subjects have the right to:

- Request what personal information the organisation holds about them and why.
- Request access to their personal information.
- Be informed how to keep their personal information up to date.

*Process to request Personal Information:*

- Access to information requests can be made by email, addressed to the Information Officer.
- The Information Officer will provide the data subject with a "Personal Information Request Form".
- Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information.
- All requests will be processed and considered against the organisation's PAIA Policy.
- The Information Officer will process all requests within a reasonable time.

**11. POPI COMPLAINTS PROCEDURE**

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

- POPI complaints must be submitted to the organisation in writing. Where so required, the Information Officer will provide the data subject with a “POPI 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 1 working day.
- The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 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 organisation’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 organisation’s governing body where after 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 organisation’s governing body within 7 working days of receipt of the complaint. In all instances, the organisation 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 may 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,
    - 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 where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPI related complaints.

**12. DISCIPLINARY ACTION**

Where a POPI complaint or a POPI infringement investigation has been finalised, the organisation 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.

In the case of ignorance or minor negligence, the organisation will undertake to provide further awareness training to the employee.

Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which the organisation may summarily dismiss the employee.

Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.

Examples of immediate actions that may be taken subsequent to an investigation include:

- A recommendation to commence with disciplinary action.
- A referral to appropriate law enforcement agencies for criminal investigation.
- Recovery of funds and assets in order to limit any prejudice or damages caused.