PROTECTION OF PERSONAL INFORMATION (POPI) POLICY	
Classification	KING PIE HOLDINGS/GEN/59
Responsible person	INFORMATION OFFICER & DEPUTY INFORMATION OFFICERS
Final Approval	MANAGING DIRECTORS
Version	2023/07
Review date	2024/07
Guideline documents	Protection of Personal Information Act, No 4 of 2013
Author	HR Manager

1. Purpose

The purpose of this policy is to ensure that the rights of all persons against the unlawful collection, retention, dissemination and use of personal information is not compromised.

In addition, this policy seeks to:

- Promote the protection of personal information processed by the company.
- Protect the rights of persons against unlawful collection, storage and dissemination of personal information.
- Establish minimum requirements for processing of personal information.
- Allocated responsibilities to certain parties to perform certain duties.
- Provide structures, systems and processes to control how personal information is handled, maintained and destroyed.
- Give effect to the right to privacy subject to justifiable use limitations aimed at protection of data related to data subjects.

2. Policy Statement

Section 14 of the Constitution of the Republic of South Africa, 1996, provides that everyone has the right to privacy;

The right to privacy includes a right to protection against unlawful collection, retention, dissemination and use of personal information

The company will respect, protect, promote and fulfill the rights in the Bill of Rights

3. Scope

The scope of this policy includes all Directors, Managers and employees in King Pie. This policy must be read in conjunction with the attached Act.

4. Version Control

This policy replaces all previous policies on use of Protection of Personal Information.

5. Personal Information

Race	**Religion/beliefs / culture**
Gender	**Language**
Sex	**Educational / financial/ employment**
Pregnancy	**ID number**
Marital status	**Email address**
National/ ethnic/ Social origin	**Physical address**
Colour	**Telephone number**
Sexual orientation	**Location**
Age	**Biometric information**
Physical or mental health	**Personal opinions, views or preferences**
Disability	**Private correspondences**

6. Special Personal Information

Information relating to a minor	**DNA**
Religious/ philosophical beliefs	**Health or sex life**
Race or ethnic origin	**Biometric information**
Trade union membership	**Criminal history**
Political persuasion	**Criminal proceedings**

7. POPI Forms to be used throughout the business

POPI General Information & Consent Form	Contains information about POPI and must be provided to all Franchisees, Employees, Suppliers, Contractors or other persons whose personal information is required for business purposes This form must be supplied to every current and future person that has any business relationship with the company Copies of all consents to be held on file – VERY IMPORTANT	K:/Company Stationery/POPI Documents
Data Subject Information Management Form: Part 1 – Request (external use)	This form to be used in the event of a request for proof, update, deletion of information we hold on a data subject	
Data Subject Information Management Form: Part 2 – Investigation (internal use)	An internal form to support the investigation request	
Personal Information Control Form	This form to be used between departments where private information is required from one party	
Training Register	Each employee (current or new) will receive training by the department head on POPI Policy and Department procedures Training for new employees on POPI, must take place during the induction phase of employment.	K:/Company Stationery/POPI Documents

	All training to be captured on the Training Register – copy to HR for the personnel files.	

8. Responsible party

King pie are the responsible party who will determine the purpose for processing Personal Information

9. Information Officer

Chief Executive Officer: Will be appointed as the Information Officer, The Information officer may decide to appoint Deputy information officers to assist with carrying out the roles and responsibilities;

Deputy Information Officers: The Information Officer will Appoint Deputy officers to assist with carrying out the roles and responsibilities of the information officer and this will be each Head of Department;

- **CFO**
- **HR Manager**
- **Legal, commercial Executive**
- **Marketing Manager**
- **Operations Executive**
- **Manufacturing Manager**
- **Retail Key Accounts Manager**

Each head of department will receive an appointment letter and on acceptance will sign an acceptance letter.

10. Definitions

Please see attached: No 4 of 2013: Protection of Personal Information Act, 2013

11. Staff Training

Senior management are responsible for ensuring that all staff in their respective departments are suitably trained in managing POPI in their own areas of work.

12. Record keeping

Senior management are responsible for ensuring that suitable mechanism are in place when it comes to keeping of records

13. (8) Conditions of the POPI Act

Condition 1: Accountability

Condition 2: Processing limitation

Condition 3: Purpose specification

Condition 4: Further processing limitation

Condition 5: Information quality

Condition 6: Quality of information

Condition 7: Security safeguards

Condition 8: Data subject participation

14. Data Subject – Rights

Data subjects is the person or company to whom personal information relates:

- Right to know if a company holds personal information
- Stop the company from using personal information
- To see what personal information the company has
- To refuse for personal information to be transferred anywhere else
- The right to say it cannot be used for certain purposes
- The right to that the personal information be changed and corrected
- The right to request that the personal information to be deleted
- The right not for decisions to be made by authorized process alone.

15. Condition 1: Accountability

Responsible parties must ensure that the conditions set out in the Act and all the measures that give effect to such conditions are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.

Senior Managers of respective departments are accountable for ensuring that all conditions in the Act are complied with.

16. Condition 2: Processing Limitation

Personal information must be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject.

Personal information may only be processed if, given the purpose for which it is processed is adequate, relevant and not excessive.

Personal information may only be processed if:

- The data subject consents to the processing
- Processing is necessary for purposes of a contact to which data subject is party
- Processing obligation is imposed by law
- Processing protects the legitimate interest of the data subject
- Processing is necessary for legitimate interests of the responsible party or third party

Senior Managers of respective departments will determine the nature and requirements of personal information processing and will ensure that the nature of information required is sufficient and not excessive and that the processing of such information complies with the requirements of the Act.

16.1 Data subject consent

The company shall provide standard consent forms to all data subjects prior to collection of any personal information

- IT Manager will ensure a folder is created on the K:drive which will be used to store all consents for all data subjects
- Such folder will contain sub-folders into which departments can save their consent forms
- Consent forms shall be saved as follows:
    - First Name/Surname/ID/Date
- Consents shall be held on file for:
    - As long as there is an active business relationship with the data subject
- Senior Managers of respective departments will ensure that standard consent forms are completed by data subjects and that these are kept on file for the period that the business relationship with the data subject exists.

16.2 Data subject request for withdrawal of consent

The company acknowledges that data subjects may withdraw their consent at any time, provided that the lawfulness of the processing of personal information before such withdrawal will not be affected.

Requests of this nature shall be directed to the Responsible party: Chief Financial Officer who will:

- Determine the reason behind such request
- Determine if the consent is still required in terms of legitimate business reason(such as other laws or business operational requirements
- Senior managers of respective departments shall ensure that where applicable that such consent is removed from all business systems and storage facilities (including but not limited to files, computers, servers and so forth)


A register of withdrawals of consent will be held on file for a period not exceeding 1 year. Such register will be held by the Senior Manager.

16.3 Data subject objection to processing of personal information

A data subject may, at any time, object to the processing of personal information, in the prescribed manner, on reasonable grounds relating to his/her situation, unless legislation provides for such processing whether data processing or for any other means.

Senior Managers of respective departments will ensure that such objections are brought to the attention of the Divisional Directors with a view to identifying alternative mechanisms suitable.


A register of such objections shall be held on file for a period not exceeding 1 year. Such register will be held by the Senior Manager.

16.4 Company processing of information where data subject has objected

The company may no longer process any personal information where a data subject has objected to such processing provided that a public law has prescribed otherwise.

Senior Managers of respective departments will ensure that such objections are brought to the attention of the Divisional Directors with a view to identifying alternative mechanisms suitable.

A register of such objections shall be held on file for a period not exceeding 1 year. Such register will be held by the Senior Manager.

16.5 Collection of personal information from data subject

Personal information must be collected directly from the data subject, unless such information is obtainable from a public record, or where such collection will not prejudice the data subject.

Note: only information that is regarded as absolutely necessary for business purposes may be collected.

17. Condition 3: Purpose specification

Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the business.

Data subjects must be made aware of the purpose of the collection of the information unless the following provisions apply:

- Where data subject has provided consent for non-compliance
- Where non-compliance would not prejudice the data subject
- Where information used would in no way identify the data subject

16.1 Retention and restriction of records

16.1.1 Retention of Records

Records of personal information must not retained any longer than is necessary for achieving the purpose related to the function or activity of the company.

Company requirements may differ dependent on the nature and reason for collection.

	Period of retention	Reason
Employee information	5 years	Legislation
Supplier information		
Franchisee information		
Competition entries		

Marketing lists		
List other types of information we may hold		

Senior Managers are responsible for ensuring that information that has reached its expiry term is deleted/remove/de-identify from all systems (electronic or hardcopy). Assessment to be performed Annually in June and then keep a record of the assessment that was performed.

16.1.2 Restriction of records

The company will ensure that processing of personal information is restricted if:

- Accuracy is contested by data subject
- The company no longer requires such information for achieving the purpose for which the information was collected
- The processing is unlawful and the data subject opposes destruction or deletion and requests restriction of use instead
- The data subject requires that the personal data be transferred into an alternative processing system.

Senior Management are required to inform the data subject before lifting any restriction on processing

16.1.3 Destruction/deletion of records

The company will ensure that destruction/deletion of all personal records will be such that no reconstruction of such records can be done.

18. Condition 4: Further processing limitation

Further processing of information must be in accordance or compatible with the purpose for which it was collected.

The following must be considered:

- Relationship between the purpose of intended further processing and the purpose for which information has been collected
- Nature of the information concerned
- Consequences of further processing for the data subject
- Manner in which information was gathered

- Contractual rights of all parties

Senior Managers are to ensure that where further processing of personal information is required, clarity is sought to the reason and purpose of such requirement.

19. Condition 5: Information quality

The Company will take the necessary and practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary.

The company will make sure that high regard is taken for the purpose of the information that will be collected and making sure that there is high regard especially if the personal information should be used for further processing based on Section 19 of the policy that refers to **Condition 4: Further processing limitation**.

20. Condition 6: Openness

The company must maintain the documentation of all processing operations under its responsibility as referred to in section 14 or 51 of the Promotion of Access to Information Act (PAIA).

19.1 Notification to data subject when collecting personal information

Where personal information is collected, the company shall inform the data subject of the following:

- The type of information being collected
- The source, if such source is not from the data subject
- The name and address of the third party
- The purpose as to why the information is required
- Whether information required from the data subject is voluntary or mandatory
- The consequences of failure to provide such information
- Any particular law authorizing or requiring the collection of the information
- Whether or not the company intends to transfer the information to a third party, country or international organisation and the level of protection of such information in that country
- Who is likely to be working/receiving such information
- Nature/Category of information
- The right of access to the information and the right to rectify such information

- The right to object to the processing of personal information
- The right to Lodge a complaint to the Information regulator and the contact details thereof
- How long such information will be held

- How such information will be destroyed.

21. Pillar 7: Security Safeguards

The company will ensure the integrity and confidentiality of personal information in its possession by taking appropriate controls, reasonable technical and organisational measures to prevent:

- Loss of and damage to, or unauthorised destruction of personal information
- Unlawful access to, or processing of personal information

20.1 Mechanisms for ensure information security

- Identify all reasonably foreseeable internal and external risks to personal information in its possession
- Establish and maintain appropriate safeguards against risks identified
- Regularly verify that the safeguards are effectively implemented
- Ensure safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards

20.1.1 Information processed by authorised operator

Anyone processing personal information may only do so on behalf of a responsible party, and in so doing only process such information with authorisation and treat such information as confidential. Operators may not disclose any personal information, unless required by law

20.1.2 Security measures regarding information processed by operator

Senior management will ensure that a written confidentiality agreement is in place for all operators

An operator must notify management immediately where there are reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by any unauthorised means.

20.1.3 Notification of security compromises

Where the company suspects that personal information of a data subject has been compromised, accessed or acquired by any unauthorised person, the company shall:

- Notify the regulator
- Notify the data subject, unless the identity of the data subject cannot be established
- Such notification must be made as soon as reasonably possible after discovery of the compromise

20.1.3.1 Notification to a data subject

The company will ensure that:

- Such notification will be mailed to the data subjects last known physical or postal address
- Sent by email to the last know email address
- Placed in prominent position on the company website
- Published in news media, or as directed by Regulator

Such notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the security breach including:

- Description of possible consequences of breach
- Description of measures that the company has or will take to address the breach
- Recommendation as to the measures to be taken by the data subject to mitigate possible adverse effects of breach
- Identity, if known of the unauthorised person who may have accessed or acquired the personal information

22. Conition 8: Data subject participation

21.1 General information

On request of the data subject, the company will provide, free of charge:

Confirmation on what information is held on the data subject

Proof, record or description of the type of personal information held about the data subject, including identity of all third parties who may have had, or have access to the information

This information will be provided within a reasonable time in a reasonable format and manner and in a form that is understandable.

21.2 Correction of information

On request of the data subject in writing, the company will delete or correct any personal information held on the data subject that may be inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or

Destroy or delete a record of personal information that the company is no longer authorised to retain

The company will, within a reasonable time correct the information, destroy or delete the information and provide to the data subject proof, to his/her satisfaction, with credible evidence that this has been done.

23. Management Responsibility

All Senior Management and Department Heads are responsible for carrying out all analysis to determine the nature of personal information held and to put into place systems, processes and procedures to ensure that the department is POPI compliant so as to avoid any contravention penalties incurred by King Pie holdings Holdings (Pty) Ltd.

Protection of Personal Information: Consent Form

In terms of the Protection of Personal Information Act, data subjects are required to provide consent for use of their personal information for business purposes.

Please read carefully through the consent clauses below.

PERMISSION TO USE YOUR PERSONAL INFORMATION

By agreeing to the terms of this consent form, I hereby voluntarily authorize **(name of company)** to process my personal information which includes but is not limited to my name, ID number, banking details, physical address, telephone numbers, email address, financial information & any other information I have provided to the company.

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

This consent is effective immediately & will endure until the relationship between myself and **(name of company)** has been terminated.

By agreeing to the terms of this consent form, I expressly consent to the processing of my information for business and/or for requirements of public law.

YOUR RIGHTS IN TERMS OF THIS CONSENT

The company notes that you have the:

- **Right to know what information is being kept,** how that information is being used & when we will disclose that information
- **Right to correct your details** – Open Doors endeavours to keep your information up to date, should any of your details have changed please notify us of same so that our records are as accurate as possible.

- **Right to revoke consent** – You may revoke your consent given to us in terms of this form at any time.

- Revoked consent is not retroactive & will not affect disclosures of your information already made.

- Revocations are to be in writing and addressed to the company POPI information Officer.

POPI Information Officer
POPI Deputy Information offices
c/o King Pie Holdings (Pty) Ltd
Box 2606, Midrand, 1686

Email: mabason@kingpie.co.za

TRANS-BORDER FLOW OF INFORMATION

Where the company consults in any trans-border business on my behalf, I expressly consent to the processing of my personal information by way of the trans-border flow of information. This will occur where personal information has to be sent to service providers outside of the Republic of South Africa for storage or further processing processes on the company's behalf. We will not send your information to another country that does not have similar information protection legislation in place.

Surname: _____First Names: _____

Date: _____

Signature: _____

ACKNOWLEDGEMENT OF RECEIPT OF POPI POLICY

I hereby confirm the following:

- ☐ I have been issued with a copy of the POPI policy
- ☐ I am aware that copy of this policy can be found on the K:/Policy and Procedures
- ☐ I understand my responsibilities with regards to the implementation, management and review of POPI procedures within my area of responsibility

Full Names: _____

Signature: _____

Date: _____