



Manual in terms of the Promotion of Access to Information Act (PAIA), and the Protection of Personal Information Act (POPIA)

Table of Contents

1. Company Details	2
2. Introduction	2
3. Scope	2
4. Contact Details	2
5. Details of Information Officer	3
6. Consent	4
7. Accountability	5
8. Processing Limitation – Purpose Specific	5
9. Limitation on Further Processing	5
10. Information Quality	5
11. Transparency/Openness	5
12. Collecting Information	5
13. Use of Information	6
14. Sharing of Information	7
15. Safeguard of Information	7
16. Access to Information	7
17. Policy Compliance	8
18. Operational Considerations	8
19. Administration of the Group Policy	8

1. Company Details

The Group is committed to business practices in compliance with all relevant legislation, which includes the Protection of Personal Information Act 4 of 2013 (“the POPIA”), once in operation, the Electronic Communications and Transaction Act 25 of 2002 (“the ECTA”), the Promotion of Access to Information Act 2 of 2000 (“the PAIA”) and the Consumer Protection Act 68 of 2009 (“the CPA”), particularly Section 11 of the CPA for the purposes of this policy.

CHESTER GROUP respects the right to privacy and confidentiality and is committed to maintaining the privacy and security of its employees, customers, suppliers and the general public (the stakeholders) information.

2. Introduction

This Manual has been prepared in respect of the CHESTER Group of Companies, which includes the following related entities:

- Chester Wholesale Meat KZN (Pty) Ltd
- Chester Butcheries (Pty) Ltd
- Humingbird Investments (Pty) Ltd
- Vamasa (Pty) Ltd
- Chandling International (Pty) Ltd
- Cape Town Ship Suppliers (Pty) Ltd
- Pasadona Investments (Pty) Ltd

This Manual excludes the Group’s operations outside of the Republic of South Africa and will serve to provide a reference regarding the records held by the Company at its Registered Office and various operations within the borders of the Republic of South Africa.

3. Scope

This policy applies to the processing of personal information by all employees, employed by the Group, all business units of the Group and all stakeholders who interact with the Company and is fully binding on all stakeholders.

Employees, business units and stakeholders are expected to be familiar with, and to comply with this policy. Failure to do so by employees may result in disciplinary action. The Company will ensure that all contracts with third parties will comply with the principles set out in this policy.

4. Contact details

Name of body: Chester Wholesale Meat KZN (PTY) LTD

Registration Number: 1998/016290/07

Postal Address: PO Box 336, Durban, 4000

Telephone Number: 031 001 9501

5. Details of Information Officer

The Information Officer of the Company is:

Mr. Nigel Oliver

Physical Address:

14-22 Watford Road

Congella

Durban

4001

Postal Address:

PO Box 336

Durban

4000

Telephone Number: 031 001 9594

E-mail: nigel@chestersa.com

We are committed to compliance with The Protection of Personal Information (POPI) Act which requires us to:

1. Sufficiently inform customers, suppliers, staff and the general public, (the Data Subjects) whose personal information we may collect and process during the ordinary course of business, the fact that we are processing their personal information and the purpose for which we process the information.
2. Protect the data that we hold from threats, whether internal or external, deliberate or accidental, to ensure that the personal information of Data Subjects is not lost, accidentally destroyed, misused or disclosed, and is not accessed, except by our Stakeholders, in the proper performance of their duties.

Our policy and compliance framework establishes measures and standards for the

protection and lawful processing of personal information within our organisation and provides principles regarding the right of individuals to privacy and to reasonable safeguarding of their personal information.

The Information Officer, is responsible for:

- Conducting a preliminary assessment.
- The development, implementation and monitoring of our policy and compliance framework.
- Ensuring that the policy is supported by appropriate documentation.
- Ensuring that documentation is relevant and kept up to date.
- Ensuring the policy and subsequent updates are communicated to relevant managers, representatives, staff, and associates, where applicable.

All employees, subsidiaries, business units, departments and individuals directly associated with us are responsible for adhering to this policy and for reporting any security breaches or incidents to the Information Officer.

Any Service Provider that requires access to our data in order to provide effective services to our organisation, must adhere to the requirements of the POPI Act, to ensure adequate protection of personal information, held or processed by them, on our behalf. Written confirmation to this effect will be obtained from the relevant service providers.

6. Consent

The supply of information to the Chester Group by any of its Data Subjects is at the discretion of the Data Subject. By supplying us with any information, Data Subjects are accepting the principles, practices and terms contained in this manual.

In respect of all marketing activities relating to the Company's services and/or products, consent to collect or use information will be obtained. Consumers will be given an option to opt-in or opt-out of any electronic communication.

In respect of other activities, consent to collect or use will be obtained via acknowledgement by the Data Subject concerned that the Group is collecting his or her personal information. This acknowledgment will be contained in all documents where personal information is collected, including any contracts concluded with the Chester Group. In certain instances, the Data Subject may be specifically requested to sign an acknowledgment of the collection of personal information.

If information is collected through a third party, the third party will be requested to sign a declaration that they comply with the POPIA requirements.

It is to be noted that The Chester Group:

- has different business units that process and share personal information internally and will share information relating to a Data Subject internally in certain instances; and
- is obliged to disclose certain categories of information for regulatory and legal purposes.

7. Accountability

We will take reasonable steps to ensure that personal information obtained from Data Subjects is stored safely and securely.

8. Processing Limitation – Purpose specific

We will collect personal information directly from Data Subjects and we will only collect relevant information for the purpose for which it is required.

Once in our possession we will only process information with the consent of the Data Subject, except where we are required to do so by law. In the latter case we will always inform the Data Subject.

9. Limitation on Further Processing

Personal information will not be processed further in a way that is incompatible with the purpose for which the information was collected initially.

We collect personal information for employment purposes and recruitment as well as for suppliers and customers, and it will only be used for that purpose.

10. Information Quality

We are responsible for ensuring that all Data Subject information is complete, up to date and accurate whilst held by the Group.

This means that it may be necessary to, from time to time, update this information and confirm that it is still relevant.

11. Transparency / Openness

Where personal information is collected from a source other than directly from the relevant Data Subject, we are responsible for ensuring that the Data Subject is aware:

- that their information is being collected,

- who is collecting their information by giving them our details, and
- the specific reason why we are collecting their information.

12. Collecting Information

The type of information collected varies. Information includes any personal information as defined in the POPIA, such as (but is not limited to): details such as name, age, ID numbers, registration numbers, addresses and other contact details, liabilities, income and payments records, financial information and banking details such as account numbers, and biometric details such as fingerprints.

Data Subject's information in general refers to information submitted to us through:

- recruitment,
- our website that identifies or relates to an online visitor or customer, whether they are an individual or a business,
- competitions,
- marketing activities. It is to be noted that for purposes of marketing campaigns, that further processing of personal information will be compatible with the original purpose of collection,
- security measures, such as image recording from video surveillance systems (if any) placed on premises belonging to the Company, including access control devices,
- agreements and/or contracts concluded with Group Companies,
- third party sources, where allowed to do so in law,
- emails,
- social media,
- registers, and
- other communications sources.

13. Use of Information

We use information to identify our customers, suppliers, employees, and others who we deal with in the ordinary course of business.

Personal information is necessary to enable us to:

- contact customers and suppliers etc.
- perform our duties in pursuance of any contract.
- comply with any regulatory or other business obligation.
- carry out market research, business, and statistical analysis.
- carry out any other reasonable business operations; and
- carry out our obligations in connection with employment of personal.

Information may also be used for other purposes for which permission is given, or if required by law, or if it is of public interest to disclose such information. We undertake to only process information that is required and relevant for the purposes set out above.

The Company will not intentionally collect information about children and will only process information about children with the consent of a parent or guardian, or if otherwise required to do so by law.

The Company does not intend to process any 'special personal information as defined in the POPIA, except as specifically allowed by POPIA. We will only process special personal information for any other purpose with the Data Subjects' express consent, or if otherwise required to do so by law.

Data Subjects may on reasonable grounds object to the processing of information, after which we undertake not to continue to process, except when required to do so by law.

Information will be retained for as long as is necessary for the purpose for it was collected, but not for less than the period required by legislation where applicable.

14. Sharing of Information

We will only share information with third parties with a Data Subjects consent or if otherwise required to do so by law.

We have trusted relationships with selected third parties who perform services on our behalf. All service providers are bound by contract to maintain the security of our Data Subjects' information and to use it only as permitted by us.

15. Safeguard of Information

We understand the value of personal information and will take all reasonable steps to protect the information from loss, misuse, or unauthorised access.

Our responsibility is to:

- protect and manage personal information that we hold about Data Subjects.
- make use of electronic and computer safeguards, such as firewalls and data encryption, to secure Data Subject's information.
- have physical and electronic access control to its premises; and
- only authorise access to information to those employees who require it to fulfil their designated responsibilities.

We are committed to using appropriate technical and other security measures in line with acceptable industry standards to safeguard Data Subject's information.

16. Access to Information

Data Subjects have the right to access their information, including certain personal information held by us. Requests for information must be made to the Information Officer:

A Data Subject, having provided adequate proof of identity, has the right to

- request a responsible party to confirm whether or not we hold personal information about the Data Subject; and
- request from us the record or a description of the personal information relating to the Data Subject that is held by us, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information.

A Data Subject may, in the prescribed manner, request us to

- correct or delete personal information about the Data Subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully; or
- destroy or delete a record of personal information about the Data Subject we are no longer authorised to retain in terms of the POPIA.

17. Policy Compliance

Any breach/es of our POPI policy may result in disciplinary action and possible termination of employment.

18. Operational Considerations

- **Monitoring**

The Management and Information Officer are responsible for administering and overseeing the implementation of our POPI policy and, as applicable, supporting guidelines, standard operating procedures, notices, consents and appropriate related documents and processes.

All employees, subsidiaries, business units, departments and individuals directly associated with us are to be trained, according to their functions, in the regulatory requirements, policies and guidelines that govern the protection of personal information.

We will conduct periodic reviews, where appropriate, to ensure compliance with our policy and guidelines.

- **Operating controls**

We shall establish appropriate standard operating procedures that are consistent with our policy and regulatory requirements. This will include:

- Allocation of information security responsibilities.
- Incident reporting and management.
- User ID addition or removal.
- Information security training and education.
- Data backup.

19. Administration of the Group Policy

The custodian of the Group policy is the Information Officer who will be responsible for the administration, revision, interpretation, and application of this policy, which will be reviewed annually or as and when required.

Any alteration of this policy is subject to approval by the Board of Directors.