DRAKENSTEIN
MUNISIPALITEIT • MUNICIPALITY • UMASIPALA
Paarl | Wellington | Gouda | Saron | Simondium

Privacy Policy

Date of Approval/Review by Council	Implementation Date
30 June 2023	30 June 2023

Signed by the City Manager	Signature Date
	30 June 2023

TABLE OF CONTENTS

1. INTRODUCTION

1.1 In order to fulfil its legislated functions and duties, Drakenstein Municipality (hereinafter referred to as "the Municipality") needs to gather, process, store, and destruct certain information about individuals and juristic persons (collectively referred to as "data subjects"). These can include clients/customers, suppliers, business contacts, employees and other people the Municipality has a relationship with or may need to contact.

1.2 This policy describes how this information must be collected, handled and stored to meet the organisation's personal information protection standards and to comply with the Protection of Personal Information Act, 2013 (Act 4/2013) (hereinafter referred to as "the Act").

1.3 This policy must be read together with the Act and Drakenstein's Records Management Policy.

1.4 Definitions appear at the end for the meaning of terms used in this policy.

2. PURPOSE

This privacy policy ensures that the Municipality:

2.1 complies with the Act;
2.2 protects the rights of data subjects;
2.3 is open about how it stores and processes personal information of data subjects; and
2.4 protects itself from the risks of a security breach.

3. POLICY STATEMENT

3.1 Drakenstein Municipality is committed to protecting the privacy of data subjects in accordance with the obligations imposed by the Act. The Act describes how organisations must collect, handle and store the personal information of data subjects. These rules apply regardless of whether the information is stored electronically, on paper or on other materials.

3.2 To comply with the Act, personal information must be collected fairly, stored safely and not disclosed unlawfully.

3.3 The Act is underpinned by the following important privacy principles. These principles state that personal information must:

3.3.1 be processed fairly and lawfully;
3.3.2 be obtained only for specific, lawful purposes;
3.3.3 be adequate, relevant and not excessive;
3.3.4 be accurate and kept up to date;
3.3.5 not be held for longer than necessary;
3.3.6 processed in accordance with the rights of data subjects;
3.3.7 be protected in appropriate ways; and
3.3.8 not be transferred outside South Africa unless that country or territory also ensures an adequate level of protection.

4. SCOPE

4.1 This policy applies to all the Municipality's employees and councillors, and any other person or entity working for or on behalf of the Municipality such as, but not limited to:

4.1.1 interns;
4.1.2 volunteers;
4.1.3 consultants; and
4.1.4 contractors, suppliers or service providers, including their staff or agents.

4.2 The policy furthermore governs all business activities that involve the processing of personal information, including special personal information, for or on behalf of the Municipality. This can include, but is not limited to:

4.2.1 names of individuals and juristic persons;
4.2.2 contact information such as postal and e-mail addresses and telephone numbers;
4.2.3 biographical information such as date of birth, race, gender and marital status;
4.2.4 any identifying number, location information or online identifier;
4.2.5 biometric information such as fingerprints; and
4.2.6 educational, medical, financial, criminal or employment history.

5. RISKS

This policy helps to protect the Municipality from certain types of security risks, including:

5.1 **Breaches of confidentiality**: for instance, information being shared inappropriately.

5.2 **Failing to offer choices**: for instance, all data subjects should be free to choose how the organisation uses information relating to them where the personal information is not collected, used or shared in terms of a law or an agreement between the data subject and the organisation.

5.3 **Reputational damage due to non-compliance on the requirements of the Act.** For instance, the unauthorised sharing of personal or confidential information by officials with persons or parties who are not entitled to such information.

6. RESPONSIBILITIES & DELEGATIONS

6.1 All staff members have the responsibility to ensure that the personal information of data subjects are collected, stored and handled appropriately to ensure the confidentiality, integrity and availability thereof.

6.2 Each Information End User, Information Owner, business unit and team that handles or processes personal information must ensure that it is handled and processed in line with this policy and the privacy principles.

6.3 Key areas of responsibility

6.3.1 The **Information Officer** is ultimately responsible for ensuring that the Municipality meets its legal obligations.

6.3.2 The Deputy Information Officer, as assigned in terms of the System of Delegations, is responsible for:

(a) keeping the Information Officer updated about information assets and personal information protection responsibilities, risks and issues;

(b) reviewing all personal information protection procedures and related policies, in line with an agreed schedule;

(c) arranging personal information protection training and advice for the people covered by this policy; and

(d) checking and approving any contracts or agreements with third parties that may collect, handle or store personal information on behalf of the organisation.

6.3.3 The Deputy Information Officer is responsible for dealing with requests from data subjects who want to see the personal information the Municipality holds about them (also called "data subject access requests"). The identity of anyone making a data subject request must be verified before disclosing any personal information.

6.3.4 The ICT Manager is responsible for:

(a) ensuring all ICT assets used for processing personal information meet capable security standards;

(b) performing regular checks and scans to ensure security hardware and software is functioning properly;

(c) evaluating any third-party services the Municipality is considering using to process personal information. For instance, cloud computing services.

6.3.5 The Senior Manager of each operator (person who processes personal information) is responsible for:

(a) identifying personal information that is or may be processed within their sections or divisions, in line with the Act;

(b) preparing and maintaining internal procedures to support the effective handling and security of personal information;

(c) reviewing all personal information protection procedures and related policies, in line with an agreed schedule and make recommendations to the Deputy Information Officer where applicable; and

(d) ensuring that all employees, consultants, service providers and others that report to such Senior Manager are made aware of and are instructed to comply with this and all other relevant policies.

6.3.6 The Information Officer or his/her delegatee is responsible for:

(a) approving any personal information protection statement attached to communications such as e-mails and letters;
(b) addressing any personal information protection queries from journalists or media outlets; and
(c) where necessary, working with other business units to ensure all communication initiatives abide by the privacy protection principles.

7. GENERAL STAFF GUIDELINES

7.1 Access to any personal information covered by this policy is only authorised for those who **require such access in order to perform their duties**.

7.2 Personal information is **under no circumstances to be shared with unauthorised persons inside or outside the Municipality** and must never be shared over social media.

7.3 When access to confidential information is required, employees can request it from their line managers.

7.4 The Municipality **will provide training** to all employees to help them understand their responsibilities when handling personal information.

7.5 Employees must keep all personal information **secure**, by taking sensible precautions and following the guidelines set out herein.

7.6 In particular, **strong passwords must be used** and they should never be shared, as regulated in terms of the ICT Master Framework.

7.7 Personal information must be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of in line with the disposal instructions.

7.8 Employees **should request help** from their line manager if they are unsure about any aspect of the protection of personal information.

7.9 Line managers should seek the assistance of Deputy Information Officer if they are unsure about any aspect of the protection of personal information.

7.10 Collection of personal information

The Municipality collects personal information to support its service delivery mandate. Personal information is collected directly from data subjects where practical and always in compliance with the Act. The types of information and the purposes for which personal information is collected is set out in the Municipality's Privacy Notice.[1]

7.11 Classification

The Operator classifies information in accordance with its legal requirements, value, criticality and sensitivity to unauthorised disclosure, modification or loss in terms of the Records Management Policy:

7.11.1 personal information is usually classified as CONFIDENTIAL; and
7.11.2 special personal information and children's information is classified as SECRET.

7.12 Use

7.12.1 When personal information is accessed and used it can be at the risk of loss, corruption or theft of such information. As an existing data protection measure, computer screens will lock within a set time whenever computers are unattended.

7.12.2 The following are required from employees:

(a) personal information may **under no circumstances be shared informally;**
(b) all personal information sent over **e-mail** (as an attachment or in an email text) must be considered sensitive and protected as such. It may not be sent to someone outside of the Municipality unless it has been approved by the Deputy Information Officer. This includes forwarding such e-mails to an employee's own personal e-mail account;

[1] Create a hyperlink to this Privacy Notice/ include details where it can be obtained.

(c) before sending an e-mail to a co-employee, confirm with the line manager that the recipient is allowed to have access thereto since not all users within the organisation have access to the same information;
(d) personal information may never be transferred outside of South Africa without the approval of the Deputy Information Officer and without assurance that the country where it is transferred will ensure an adequate level of protection of personal information;
(e) employees may not save copies of personal information to their own computers. Such information may only be saved on a designated drive;
(f) employees that require personal information data to be copied to their own computers or other storage media, for operational reasons, may only do so with the prior written permission of the Deputy Information Officer.

7.13 Storage

7.13.1 These rules describe how and where personal information should be safely stored. When personal information is **stored on paper**, it must be kept in a secure place where unauthorised people cannot have access to it. These guidelines also apply to personal information that is usually stored electronically but has been printed out for some reason:

(a) when not required, the paper or files should be kept **in a locked drawer or filing cabinet.** Where the information is classified as **SECRET access** to the environment should be **restricted** and logged;
(b) employees must ensure that paper and printouts are **not left where unauthorised people could see them**, like on a printer or photocopier;
(c) **printouts that contain personal information should be shredded immediately** and disposed of securely when no longer required;

7.13.2 When personal information is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

(a) all electronic storage requires access controls equal to those in production and file protection mechanisms such as password control as regulated in terms of the ICT Master Framework;

(b) audit trail data must be available on all information and application system activities;

(c) personal information may only be stored on **designated storage media;**

(d) storing personal information on any other physical devices, including but not limited to USB drives (memory sticks), external hard drive, CD or DVD must be **pre-approved** by the Deputy Information Officer;

(e) if personal information is **stored on removable media** (like a memory stick, external hard drive, CD or DVD) the files must be password protected and the media must be locked away securely when not being used;

(f) electronic files and designated drives that contain personal information will be **backed up frequently** as regulated in terms of the ICT Master Framework; and

(g) all servers, computers and other electronic devices containing personal information should be protected by **approved security software and a firewall.**

7.14 Data accuracy

7.14.1 The Act requires the Municipality to take reasonable steps to ensure personal information is kept accurate and up to date. It is the responsibility of all employees who work with personal information to take reasonable steps to ensure that it is kept as accurate and up to date as possible.

7.14.2 Electronic files that contain personal information will be held in **as few places as necessary.** Staff should not create any unnecessary additional data sets.

7.14.3 Staff should **take every opportunity to ensure personal information is updated as far as practically possible.**

7.14.5 Personal information should be **updated as inaccuracies are discovered.** For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

7.15 Disposal

7.15.1 Working papers and copies that may be disposed of in terms of a general disposal instruction must be disposed of by using a secure disposal container or shredder.

7.15.2 The disposal of all original files and electronic files must be performed in accordance with the Municipality's Records Management Policy.

8. DATA SUBJECT ACCESS REQUESTS

8.1 If a data subject contacts the Municipality requesting this information this is called a data subject access request.

8.2 All data subjects whose personal information is held by the organisation are entitled to:

8.2.1 ask **what information** the organisation holds about them, why and with who it is shared;
8.2.2 ask **how to gain access** to it;
8.2.3 be informed **how to keep it up to date; and**
8.2.4 be informed how the organisation is **meeting its obligations in terms of POPIA.**

8.3 Access requests from data subjects must be referred to the Deputy Information Officer.

9. DISCLOSING (SHARING) PERSONAL INFORMATION

9.1 Internal disclosure

In general, personal information is shared within the organisation where legally permitted for reasonable and appropriate business purposes. However, even within the organisation access is restricted to only those employees or third parties who need access to carry out their assigned functions.

9.2 External disclosure

9.2.1 External to the organisation disclosure is only made pursuant to an agreement, as permitted or required by law or legal process, or with the written consent of the data subject.

9.2.2 POPIA allows personal information to be shared if it involves national security or criminal activities without the consent of the data subject. Under these circumstances the requested personal information will be disclosed. However, the Deputy Information Officer will ensure that the request is legitimate and in line with POPIA, seeking assistance from Legal Services Section, where necessary.

10. NOTIFICATION TO DATA SUBJECTS

10.1 The organisation aims to ensure that data subjects are aware that their personal information is being processed, and that they understand how the personal information is being used, what their rights are in terms of POPIA and how to exercise their rights.

10.2 To these ends, the organisation has a privacy notice, setting out how personal information relating to a data subject is collected and used by the organisation.

10.3 This is available on request. A version of this notice is attached as ANNEXURE A and is also available on the Drakenstein Municipality webpage.

11. ENFORCEMENT

11.1 Non-compliance with this policy by the Municipality's employees will be dealt with in accordance with the Disciplinary Code of the organisation. Consequences may include disciplinary action up and to termination of employment, and/or legal proceedings to recover any loss or damage to the organisation, including the recovery of any fines or administrative penalties imposed by the Information Regulator on the organisation in terms of POPIA.

11.2 Non-compliance with the policy by any other third party processing personal information on behalf of the organisation will be dealt with in accordance with the agreement entered into between the organisation and such third party. Consequences may include the recovery of any fines or administrative penalties imposed by the Information Regulator on the organisation in terms of POPIA or termination of agreement.

12. REVIEW AND UPDATE

12.1 This policy will be reviewed and updated as and when required.

12.2 If any regulatory or business changes result in a significant addition or change to the nature or handling of personal information that may require a review of this policy the changes will be developed by the Legal Services Section of the Municipality.

12.3 Any questions and requests to update the policy should be directed to the Executive Director: Corporate and Planning Services.

DEFINITIONS	
Data subject	Means the identifiable natural/juristic person to whom personal information relates.
Information assets	Means the assets the Municipality uses to create, store, transmit, delete and/or destroy information to support its business activities as well as the information systems with which that information is processed. It includes: • All electronic and non-electronic information created or used to support business activities regardless of form or medium, for example, paper documents, electronic files, voice communication, text messages, photographic or video images. • All applications, devices and other systems with which the organisation processes its information, for example telephones, fax machines, printers, computers, networks, voicemail, e-mail, instant messaging, smartphones and other mobile devices ('ICT assets').
Information end user	Means a person that interacts with information assets and ICT assets for the purpose of performing an authorised task.
Information officer	Means the Accounting Officer.
Information owner	Means a person/staff member responsible for, or dependent upon the business process associated with an information asset.
Personal information	Means information relating to an identifiable, living, natural person, and were it is applicable, an identifiable, existing juristic person, including, but not limited to: a) Information relating to the race, gender, marital status, nationality, age, physical or mental health, disability, belief, culture, language and birth of the person; b) Information relating to the education or the medical, financial, criminal or employment history of the person; c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person d) the biometric information of the person; e) the personal opinions, views or preferences of the person; f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

	g) the views or opinions of another individual about the person; and h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.
Processing	Means any operation or activity or any set of operations concerning personal information, including: a) the collection, receipt, recording, organisation, collation, storage, updating, modification, retrieval, alteration, consultation or use; b) dissemination by means of transmission, distribution or making available in any other form; or c) merging, linking, as well as restrictions, degradation, erasure or destruction of information.
Special personal information	Means personal information as referred to in section 26 of POPIA.

Condensed Privacy Notice

Privacy notice – short version
Drakenstein Municipality respects and protects your privacy

What is this notice for and who does it apply to?

This notice briefly explains how Drakenstein Municipality collects and uses personal information.

We collect personal information from or about citizens, employees and suppliers

- The Municipality collects the minimum personal information required for the purpose of fulfilling its role as employer, business partner and/or service provider.
- It collects only the personal information you choose to provide us with as a member of the public, job applicant, employee or supplier.
- The Municipality also collects information needed to provide specific public services.
- Other sources such as service providers or public bodies may also collect or check information from or about you on behalf of the Municipality.

Types of personal information we collect and use

- The Municipality collects all or some of the following personal information where you provide it or may be typically required in certain situations:
  - general personal and contact information such as name, address, phone number and email address;
  - more detailed or sensitive information such as race, disability, gender, health and other information that is relevant and necessary to our relationship or specific government services provided;
  - educational, employment, financial and criminal history from job applicants, tax numbers, bank account details and other relevant information from employees and suppliers; and
  - close circuit television (CCTV) images, audio recordings, photographs, fingerprints and identity numbers of people who access the Municipal buildings and facilities.
- The website collects basic information about use (see website privacy notice).

Why and how the Municipality collect and use personal information

- The Municipality uses personal information routinely to communicate and manage relationships, to provide public services, for administrative reasons and to manage building security and access control.
- It only shares personal information on a confidential or restricted basis with selected:
  - external service providers working on behalf of the Municipality, and
  - staff or external bodies for historical, statistical or research purposes.
- Sometimes the Municipality is obliged to share personal information with public bodies for legal, law enforcement, public services, compliance, safety and similar reasons.
- The Municipality may store certain personal information in secure foreign data centres.

Your choices and consent in connection with your personal information

- You do not have to give us personal information, but then we may not be able to communicate with or provide public services to you.

- You have certain rights to access, correct or object to use of your personal information, subject to proof of identity.

Laws that apply to personal information and your rights

- The Protection of Personal Information Act 2013 (POPIA) and other laws regulate how the Municipality use and protect personal information.
- You may contact the Information Regulator at inforeg@justice.gov.za for help.

How to contact us to complain or ask questions

- **Email:** customercare@drakenstein.gov.za
- **Phone:** 021 807 4500
- **Post:** Civic Centre, Berg River Boulevard, Paarl, 7646
- **Visit us in person:** Civic Centre, Berg River Boulevard, Paarl, 7646