SWARTLAND MUNICIPALITY

PRIVACY POLICY

Council Resolution …….. dated ……..

TABLE OF CONTENTS

Contents

1. DEFINITIONS 1
2. INTRODUCTION 2
3. POLICY STATEMENT 2
4. SCOPE 2
5. PROVISION OF PERSONAL INFORMATION 3
6. COLLECTION OF PERSONAL INFORMATION 3
7. CATEGORIES OF PERSONAL INFORMATION THE MUNICIPALITY MAY USE AN PROCESS 4
8. SENSENTIVE INFORMATION 4
9. REASONS FOR KEEPING PERSONAL INFORMATION 5
10. SHARING PERSONAL INFORMATION 5
11. THIRD PARTY INSURANCE 6
12. SAFEGUARDING OF PERSONAL INFORMATION 6
13. DATA ACCURACY 6
14. DATA MINIMISATION 6
15. RETENTION OF PERSONAL INFORMATION 7
16. DATA SUBJECTS RIGHT TO ACCESS AND MANAGE PERSONAL INFORMATION 7
17. MUNICIPAL WEBSITE 7
19. RESPONSIBLITIES 8
20. POPIA COORDINATING COMMITTEE 9
21. GENERAL STAFF GUIDELINES 10
22. BREACHES OF THE ACT OR POLICY 11
23. MAINTENANCE AND UPDATING OF THE PRIVACY POLICY 11
24. INFORMATION OFFICER AND CONTACT DETAILS 11

1. DEFINITIONS

Data subject	Means the identifiable natural/juristic person to whom personal information relates.
Information assets	Means the assets the organisation 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 content. • 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 custodian	Means the person responsible for defining and implementing security measures and controls for Information and Communication Technology ('ICT') assets.
Information end user	Means the person that interacts with information assets and ICT assets for the purpose of performing an authorised task.
Information officer	Means the Accounting Officer/ Municipal Manager
Information owner	Means the person 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 where 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.

2. INTRODUCTION

(1) The Swartland Municipality ("Municipality") needs to gather and use certain information about individuals and juristic persons (collectively referred to as "data subjects"). These can include clients/customers, suppliers or service providers, business contacts, employees and other people the Municipality has a relationship with or may need to contact.

(2) The policy ensures that the Municipality:
- (a) Complies with the Protection of Personal Information Act, 2013 (Act 4 of 2013) (POPIA).
- (b) Protects the rights of data subjects.
- (c) Is open about how it stores and processes personal information of data subjects.
- (d) Protects itself from the risks of security breaches in any form.

(3) The policy is available on the Municipality's website and at municipal offices in the municipal area.

3. POLICY STATEMENT

(1) The Municipality is committed to protecting the privacy of data subjects in accordance with the obligations imposed by POPIA. POPIA describes how organisations must collect, handle and store the personal information of data subjects.

(2) These rules apply regardless of whether the information is stored electronically, on paper or on other materials.

(3) POPIA is underpinned by the following important privacy principles. These state that personal information must:
- (a) be processed fairly and lawfully;
- (b) be obtained only for specific, lawful purposes;
- (c) be adequate, relevant and not excessive;
- (d) be accurate and kept up to date;
- (e) not be held for longer than necessary;
- (f) processed in accordance with the rights of data subjects;
- (g) be protected in appropriate ways;
- (h) not be transferred outside South Africa unless that country or territory also ensures an adequate level of protection.

4. SCOPE

(1) The Policy applies to all municipal employees, councillors, customers/clients and all external parties with whom we interact, including but not limited to our consultants, agents, individuals, representatives of organisations, visitors to our offices and visitors to our website and social media platforms.

(2) The Municipality collect personal information for various reasons in order to fulfil its mandate as government institution in terms of the Constitution of the Republic of South Africa. The residents expecting essential and other services from the Municipality are obliged to share their personal information with the Municipality as the withholding and/or refusal of personal information may impact on the Municipality`s ability to render effective and sufficient services.

(3) Employees are also obliged to share their personal information with the Municipality as it is needed for human resource management.

5. PROVISION OF PERSONAL INFORMATION AND CONSENT

(1) By providing the Municipality with your personal information, you:

(a) agree to the terms and conditions set out in the Privacy Policy and authorise the Municipality to retain, process, use and disseminate such information as set out herein, and;

(b) authorise the Municipality**,** its staff, members, service providers and other third parties to use, disseminate and process your personal information for the purposes stated in the Policy.

(2) The Municipality will not use your personal information for any other purpose than that is set out in the Policy and will endeavour to protect your personal information that is in the Municipality's possession, from unauthorised alteration, loss, disclosure, use, dissemination, or access.

(3) Please note that the Municipality may review and update the Policy from time to time. The latest version of the Policy is available on request, free of charge, at the municipal offices and available on the Municipality's website. See our contact details herein below.

6. COLLECTION OF PERSONAL INFORMATION

(1) The Municipality collects information to support its service delivery mandate. We will process your personal information in the ordinary course of the Municipality's business. We will primarily use your personal information only for the purpose for which it was originally or primarily collected.

(2) The Municipality may collect of obtain personal information about you/our clients/customers:

(a) directly from you;

(b) in the course of our relationship with you/our customers/clients;

(c) when you make your personal information public;

(d) when you visit and/or interact with the municipal website at www.swartland.org.za or Facebook social media platform;

(e) when you register to use any of our services;

(f) when you attend any activity and/or event of whatsoever nature at the Municipality and/or presented and/or organized by the Municipality;

(g) Through surveillance cameras (with facial recognition technology);

(h) License Plate Recognition cameras;

(i) when you visit our offices.

(3) The Municipality may also receive personal information about you from third parties (eg, law enforcement authorities).

(4) In addition to the above, the Municipality may create personal information about you such as records of your communications and interactions with us, including, but not limited to, electronic communications, your attendance at events or at interviews in the course of applying for a job with us, subscription to our newsletters and other mailings and interactions with you.

7. CATEGORIES OF PERSONAL INFORMATION THE MUNICIPALITY MAY USE AND PROCESS

(1) Depending on the nature of the services required, the relationship between the individual and the Municipality and the reasons why certain information is required, personal information that may be obtained includes but is not limited to:

(a) personal details: full name and surname, photographs, video material;
(b) biographical information: date of birth, race, gender and marital status;
(c) demographic information: gender, date of birth/age, nationality, culture, ethnicity, religion, salutation, title, and language preferences;
(d) biometric information: finterprinting, retinal scanning, voice recognition;
(e) employment information: remuneration details, qualifications, medical information, declaration of interest;
(f) identifier information: passport or national identity number; ;
(g) contact details: correspondence address, telephone number, mobile number, email address, and details of your public social media profile(s);
(h) attendance records: details of meetings and other events organised by or on behalf of the Municipality that you may and/or may not have attended;
(i) consent records: records of any consents you may have given, together with the date and time, means of consent and any related information;
(j) payment details: billing address; payment method; bank account number or credit card number; invoice records; payment records; SWIFT details; IBAN details; payment amount; payment date; and records of cheques and EFT payments;
(k) data relating to your visits to our Website and or social media platforms, your device type; operating system, browser type, browser settings, IP address, language settings, dates and times of connecting to a Website and/or social media platform, and other technical communications information.

8. SENSITIVE PERSONAL INFORMATION

(1) Where and when the Municipality need to process, disseminate and/or use your sensitive personal information, we will do so in the ordinary course of the operation of the Municipality, for a legitimate purpose, and in accordance with applicable law.

(2) The Municipality do not intentionally collect or use personal information of children (persons under the age of 18 years), unless with express consent of a parent or guardian and/or if the law otherwise allows or requires us to process such personal special information.

9. REASONS FOR KEEPING PERSONAL INFORMATION

(1) The Municipality may keep and process personal information for the following reasons:

a) Employment and remuneration and other Human Resource's needs;
b) Process benefits i.e. medical aid and pension;
c) Considering bids in terms of tenders and quotations;
d) Closing of agreements and contracts;
e) Communication, sending and sharing of important information;
f) Maintaining data base for essential services, indigent support, housing;
g) Respond to inquiries, complaints and requests;
h) Addressing and understanding the needs and priorities of the community and other stakeholders;
i) Security background checks (vetting);
j) Rendering accounts;
k) Debt recovery;
l) Reports to council regarding outstanding debt;
m) Audit reports.

(2) The Municipality will use your personal information for a secondary purpose only if such purpose constitutes a legitimate interest and is closely related to the original or primary purpose for which the personal information was collected.

(3) The Municipality shall not avail personal information to unaffiliated third parties for direct marketing purposes or sell, rent, distribute, or otherwise make personal information commercially available to any third party.

10. SHARING PERSONAL INFORMATION

(1) As a principle, the Municipality shall only share personal information if the Municipality has obtained consent from the data subject.

(2) Personal information may be shared with the indicated stakeholders and in the manner as follows:

(a) If required by law;
(b) Legal and regulatory authorities, upon request, or for the purpose of reporting any action or suspected breach of applicable law and/or regulation;
(c) Where it is necessary for the purposes of, or in connection with, actual or threatened legal proceedings or establishment, exercise or defence of legal rights;
(d) To any relevant party for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the executing of criminal penalties, including, but not limited to safeguarding against, and the prevention of threats to public security;
(e) To any relevant party for human resources purposes such as SARS, medical aid funds, pension funds, financial institutions;
(f) Business partners, vendors, or contractors to provide requested services or facilitate transactions;
(g) Where necessary to comply with judicial proceedings, court orders;
(h) To protect the rights, property, or safety of the Municipality or others, or as otherwise required by an applicable law; and
(i) Where consent in writing has been obtained from the data subject for sharing.

11. THIRD PARTY INSURANCE

(1) Any service providers with whom the Municipality shares personal information are contractually required to implement suitable information protection and security measures. Third parties are not permitted to use personal information for any purpose, other than it was intended for.

12. SAFEGUARDING OF PERSONAL INFORMATION

(1) The Municipality implements appropriate technical and organisational security measures to protect our customers/clients' personal information that is in our possession against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, unauthorised access, in accordance with applicable law. The Municipality keep hard copies and documentation containing personal information, under safe lock and key to which only authorized persons have access to. Electronic data is protected by regular password changes and firewalls.

(2) Where there are reasonable grounds to believe that your personal information that is in our possession has been accessed or acquired by any unauthorised person, the Municipality will notify the relevant Regulator and you, unless a public body responsible for detection, prevention or investigation of offences or the relevant regulator informs us that notifying you will impede a criminal investigation.

(3) Because the internet is an open system, the transmission of information via the internet is not completely secure. Although we will implement all reasonable measures to protect your personal information that is in our possession, we cannot guarantee the security of any information transmitted using the internet and we cannot be held liable for any loss of privacy occurring during the course of such transmission.

(4) When you are using our website or other social media platforms you could be directed to other sites that are beyond our control. We are not responsible for the content or the privacy policies of those third party websites.

(5) The Municipality have robust security controls and further threat detection solutions in place.

13. DATA ACCURACY

(1) The personal information provided to the Municipality should be accurate, complete and up-to-date. Should personal information change, the onus is on the provider of such data to notify the Municipality of the change and provide the Municipality with the accurate data.

14. DATA MINIMISATION

(1) The Municipality will restrict its processing of personal information to data which is sufficient for the fulfilment of the primary purpose and applicable legitimate purpose for which it was collected.

15. RETENTION OF PERSONAL INFORMATION

(1) The Municipality shall retain personal information for as long as it is necessary to fulfil the purposes for which it was collected and to comply with any legislative and or archive requirements whereafter it shall be deleted/disposed of. Depending on the purpose, retention periods shall vary.

(2) The following criteria will determine retention periods:
   (a) Legal or contractual, or other obligations to retain personal data;
   (b) Data necessary for or as part of an investigation or for litigation purposes; and;
   (c) in order to maintain accurate records, in line with relevant legislation.

16. DATA SUBJECTS RIGHT TO ACCESS AND MANAGE PERSONAL INFORMATION

(1) The data subject may request the Municipality to access, correct, update, block, or delete personal information that the Municipality holds, subject to legislative requirements that make it compulsory for the Municipality to keep such personal information.

(2) The Information Officer will acknowledge receipt of any such request within three (3) days of the date of submission.

(3) Any such requests will be dealt with by the Information Officer who shall respond within a reasonable period and no later than thirty (30) days of the date of the request.

(4) The data subject may object to the processing of personal data at any time.

(5) On any suspicion that personal information has been unlawfully processed and rights relating to protection of your personal information were violated or that personal information has been compromised, the data subject shall contact the Information Officer and if not satisfied, may lodge a complaint with the Information Regulator.

(6) In the event of an information breach that the Municipality becomes aware of, the Municipality shall notify the data subject.

17. MUNICIPAL WEBSITE

By using the Swartland Municipal website, the user is deemed to have accepted the terms and conditions as specified on the website. Other sites can be accessed via links from the website. These sites are not monitored, maintained or controlled by the Municipality and thus the Municipality are not responsible in any way for any of their contents. It is possible that the website from time to time may contain links to other third-party websites. The Municipality is not responsible for any third-party content or privacy statements. The use of such sites and applications is thus subject to the relevant third-party privacy policy statements.

The Swartland Municipal website respects any user's privacy. Some anonymous information about the user is automatically collected by the website. This information may include: the users browser type, access times, referring web site addresses and viewed pages. This information is collected to generate general aggregate statistics about the use of the Municipal website and is used to improve service delivery.

The Municipality's website may also use a "cookie" to save the users language preference. A cookie is a text file that is placed on the user's hard disk by a webpage server. Cookies cannot be used to run programmes or deliver viruses to the user's computer. Cookies are uniquely assigned to the user and can only be read by a web server in the domain that issued the cookie to the user.

The user can accept or decline cookies. Most web browsers automatically accept cookies, but the user can usually modify the browser settings to decline cookies if the user prefers. If a user chooses to decline cookies, the user's language choice will not be automatically selected each time the user returns to the website. No other cookies besides the language cookie may be used by the Municipality's website.

No other information is collected by the Municipality's website without the user's knowledge. The Municipality will not pass on any individual user details that may have been obtained, automatically or without the user's knowledge, unless the user's prior consent. The Municipality only shares anonymous aggregate statistics about users and traffic patterns.

The Municipality is not responsible for any breach of security or for the actions of third parties.

18. RISKS

(1) The Policy helps to protect the Municipality from some very real security risks, including:
   (a) Breaches of confidentiality: For instance, information being given out inappropriately;
   (b) 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;
   (c) Reputational damage: For instance, the organisation could suffer if hackers successfully gained access to the personal information of data subjects.

19. RESPONSIBLITIES

(1) All municipal employees have a responsibility to ensure that the personal information of data subjects is collected, stored and handled appropriately to ensure the confidentiality, integrity and availability thereof.

(2) Each Information End User, Information Owner, Municipal Department that handles personal information must ensure that it is handled and processed in line with the Policy and the privacy principles.

(3) Below follows key positions and their areas of responsibility:
   (a) The Information Officer (Municipal Manager) is ultimately responsible for ensuring that the organisation meets its legal obligations;
   (b) The Deputy Information Officers is responsible for:
      (i) The encouragement of compliance, by the Directorate under his/her responsibility, with the conditions for the lawful processing of personal information;
      (ii) Dealing with requests made to the Municipality relating to the directorate under his/her responsibility, pursuant to the Act;
      (iii) Working with the Regulator in relation to investigations conducted pursuant to Chapter 6 in relation to the directorate under his/her control;
      (iv) Otherwise ensuring compliance by the relevant directorate with the provisions of the Act or otherwise as may be prescribed in terms of the Act.
   (c) Apart from the responsibilities listed in subparagraph (b) above, the Director: Corporate Services is responsible for:

(i) Keeping the Information Officer updated about information assets and personal information protection responsibilities, risks and relating issues;
(ii) Reviewing all personal information protection procedures and related policies, in line with an agreed schedule;
(iii) Arranging personal information protection training and advice for the people covered by the Policy;
(iv) Checking and approving any contracts or agreements with third parties that may collect, handle or store personal information on behalf of the organisation.

(d) The ICT Manager is responsible for:
(i) Ensuring all ICT assets used for processing personal information meet capable security standards;
(ii) Performing regular checks and scans to ensure security hardware and software is functioning optimally;
(iii) Evaluating any third-party services, the organisation is considering using to process personal information. For instance, cloud computing services.

(e) The Information Owner is responsible for:
(i) Classifying personal information in line with the POPI Act and Regulations;
(ii) Maintaining internal procedures to support the effective handling and security of personal information;
(iii) Reviewing all personal information protection procedures and related policies, in line with an agreed schedule and make recommendations to the Information Officer/ Director: Corporate Services where applicable;
(iv) Ensuring that all employees, consultants and others that report to the Information Officer/ Director: Corporate Services are made aware of and are instructed to comply with this and all other relevant policies.

(f) The Communication Officer is responsible for:
(i) Approving any personal information protection statement attached to communications such as e-mails and letters;
(ii) Addressing any personal information protection queries from journalists or media outlets;
(iii) Where necessary, working with other business units to ensure all communication initiatives abide by the privacy protection principles.

20. POPIA COORDINATING COMMITTEE

(1) A POPIA-Coordinating Committee must be established to ensure the coordination of the POPIA compliance tasks and personal information requests. The Committee members will be formally appointed by the Information Officer.

(2) The Committee shall be multi-disciplinary and meet on a quarterly basis. The committee shall consist of the following portfolios:

Core Members:

- Performance & Compliance Management
- Information & Communication Technology (ICT)
- Media & Communications
- Risk Management

Departmental Representatives:

- Human Resources
- Town Planning
- Administration
- Revenue Services
- Salaries
- Supply Chain Management
- Community Services
- Infrastructure Services

Standing Invitees:

- Director: Corporate Services
- Internal Audit Representative

21. GENERAL STAFF GUIDELINES

(1) The only people able to access any personal information covered by the Policy should be those who need it to successfully complete their municipal duties.

(2) Personal information should not be shared informally and must never be shared over social media accounts such as Facebook, LinkedIn, Google Plus, etc.

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

(4) The Municipality will provide training to all employees in order to facilitate the understanding of their responsibilities when handling personal information.

(5) Employees should keep all personal information secure, by taking sensible precautions and following the guidelines set out herein.

(6) In particular, strong passwords must be used and they should never be shared.

(7) Personal information should not be disclosed to unauthorised individuals, either within the Municipality or externally.

(8) Personal information must be reviewed regularly and updated if it is found to be outdated. If no longer required, it should be deleted and disposed of in line with the disposal instructions.

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

(10) Line managers should seek the assistance of the Director: Corporate Services (Legal Services) if they are unsure about any aspect of the protection of personal information.

22. BREACHES OF THE ACT OR POLICY

Breach of the Act, either by a councillor or employee, can lead to disciplinary action against the alleged perpetrator in terms of the applicable code of conduct or disciplinary procedures.

Non-compliance with the Policy by the organisation'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.

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.

23. MAINTENANCE AND UPDATING OF THE PRIVACY POLICY

The Municipality will maintain and regularly update the Privacy Policy and shall post updated and revised versions as and when necessary.

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 the Policy the changes will be developed by the Director: Corporate Services and approved by the Information Officer.
Any questions and requests to update the policy should be directed to the Director: Corporate Services.

24. INFORMATION OFFICER AND CONTACT DETAILS

The Municipal Manager, as assigned **Information Officer** in terms of the Act, is ultimately responsible for ensuring that the organisation meets its legal obligations.

The following Deputy Information Officers will be formally appointed by the Information Officer and registered with the Information Regulator:

- Director: Corporate Services
- Manager: Secretariat and Records Services
- Snr Manager: Human Resources
- Director: Financial Services
- Manager: Credit Control
- Director: Development Services
- Director: Protection Services
- Director: Civil Engineering Services

Any questions, complaints or recommendations relating to the Privacy Policy may be directed to the Information Officer at the contact details below:

The Municipal Manager, J J Scholtz
Email: swartlandmun@swartland.org.za
Phone: 022 487 9400
Street Address: 1 Church Street, Malmesbury, 7300
Postal Address: Private Bag X52, Malmesbury, 7299