



WEST COAST DISTRICT MUNICIPALITY
PROTECTION OF PERSONAL INFORMATION POLICY

In terms of the Protection of Personal Information Act no. 4 of 2013 as amended
Government Gazette 43461 dated 22 June 2020

TABLE OF CONTENTS

	Definitions	4
1.	Introduction	6
2.	Purpose	6
3.	Objective	7
4.	Scope	7
5.	List of Personal Information	7
6.	Processing of Information	8
6.1	Limitations of processing	9
7.	Responsibilities	9
8.	General Staff Guidelines	11
9.	Quality of Information	11
10.	Documentation	11
11.	Collection of Personal Information	11
12.	Reasons for keeping personal information	12
13.	Utilisation of Personal Information	12
14.	Sharing Personal Information	12
15.	Third Party Insurance	13
16.	Safeguarding of Personal Information	13
17.	Public Participation and Service Delivery Communications	13
18.	Data Subjects: Request to access and manage Personal Information	13
19.	POPIA Complaints Procedure	14
20.	Breaches of the Act or Policy	14
21.	Municipal Website	15
22.	Retention of Personal Information	15
23.	Breaches of the Act or Protection of Personal Policy	15
24.	Monitoring and Enforcement	

DEFINITIONS

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.
Consent	Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
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.
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 The Municipal Manager appointed in terms of section 82 of the Local Government: Municipal Structures Act, 1998 (Act 117 of 1998), or the person who is acting as such.
Information owner	Means the person responsible for, or dependent upon the business process associated with an information asset.
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.

Personal information	<p>Means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to –</p> <ul style="list-style-type: none"> 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.
Record	<p>Means any recorded information, regardless of form or medium, including:</p> <p>Writing on any material;</p> <p>Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;</p> <p>Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;</p> <ul style="list-style-type: none"> 1. Book, map, plan, graph or drawing; 2. 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.
Responsible party	<p>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, the organisation is the responsible party.</p>
Special personal information	<p>Means personal information as referred to in section 26 of POPIA.</p>

PAIA	Promotion of Access to Information Act (2/2000)
PoPIA	Protection of Personal Information Act (4/2013) as amended Government Gazette 43461 dated 22 June 2020

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 ("POPIA") as amended Government Gazette 43461 dated 22 June 2020.

The Protection of Personal Information Act (POPIA), Act No. 4 of 2013, 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. POPIA regulates all organisations who process personal information. Personal information relates to information about employees, customers, suppliers and service providers.

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. The West Coast District Municipality regard the protection of personal information very important and wish to ensure that all personal information kept by the municipality is effectively safeguarded.

2. PURPOSE

The purpose of this policy is to incorporate the requirements of the Protection of Personal Information Act (4/2013) (hereafter referred to as 'PoPIA') into the daily operations of the Municipality and to ensure that these requirements are documented and implemented in municipality.

1. give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at—
 - a. balancing the right to privacy against other rights, particularly the right of access to information; and
 - b. protecting important interests, including the free flow of information within the Republic and across international borders;
2. regulate the manner in which personal information may be processed;
3. provide persons with rights and remedies to protect their personal information from processing that is not in accordance with this Act; and
4. establish voluntary and compulsory measures, including the establishment of an Information Regulator, to ensure respect for and to promote, enforce and fulfil the rights protected by this Act.

This policy ensures that the municipality:

- i. Complies with the Protection of Personal Information Act, 2013 (Act 4 of 2013) (POPIA).
- ii. The Municipality recognises privacy as a valuable human right.
- iii. Implementing internal controls for the managing the compliance risk associated with the protection of personal information.
- ii. Protects the rights of data subjects.
- iii. Is open about how it stores and processes personal information of data subjects.
- iv. Protects itself from the risks of security breaches in any form.
- v. Raising awareness through training and providing guidance who process information.

3. OBJECTIVE

The objective of this policy is to ensure the constitutional right to privacy, with regards to:

- a) the safeguarding of personal information;
- b) the regulation and processing of personal information;
- c) the execution of the prescribed requirements for the legal processing of personal information; and
- d) the protection of free flow of personal information.

The West Coast DM and its employees shall adhere to this policy concerning the management of all personal information received from, but not limited to natural persons, employees, councillors, clients, suppliers, agents, representatives to ensure compliance is applied to this Act and the applicable regulations and rules relating to the protection of personal information is adhered to.

4. SCOPE

This policy applies to all Councillors, Municipal Employees (permanent / contract) and any other person or entity working for or on behalf of the municipality. It governs all business activities that involve the processing of personal information, including special personal information, for or on behalf of this organisation.

5. LIST OF PERSONAL INFORMATION

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 in terms of Schedule 84 of the Local Government: Municipal Structures Act, Act 117 of 1998.

Employees are also obliged to share their personal information with the municipality

as it is needed for human resource management.

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

- a) Forenames and last names;
- b) Identification or Passport number;
- c) Demographic information such as age, gender, physical and postal address;
- d) Marital status, number of dependants
- a) Contact details; financial information, banking details
- b) Remuneration details;
- c) Biometric and Geographic information;
- d) Qualifications; Employment information;
- e) Ownership or rental information;
- f) Vehicle details i.e. vehicle number plate;
- g) Medical information;
- h) Declaration of interest;
- i) Next of Kin information; and
- j) Bidders information etc.

6. PROCESSING OF INFORMATION

The procedure of processing the personal information, refers to the collection, recording, organisation, storage, updating or modification, retrieval, consultation, use, dissemination by means of transmission, distribution or making available in any other form, merging, linking, including inaccessibility, erasure or destruction of personal information.

Inform the data subject what the purpose is for the collection of this information and inform the data subject regarding:

- I. whether the information to be collected is a voluntary or mandatory function to be performed;
- II. the consequences of the matter for the data subject should they fail to provide the information;
- III. whether it is ascertained that a legal authority requires the collection of the information for their records;
- IV. whether this information needs to be transferred to another source;

6.1 Limitations of processing

West Coast District Municipality will ensure that personal information will be processed in a:

- a) specific, defined and lawful manner;
- b) ensure that the data subject is aware of what information is collected prior to the collection thereof;
- c) ensure the data subject, or should the individual be a minor, a competent person in this instance then consents to the collection of personal information

7. RESPONSIBILITIES

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.

Each Department / Official that handles personal information must ensure that it is handled and processed in line with this policy and the privacy principles.

Information Officers are identified in the West Coast District Municipality Section 14 PAIA Manual as gazetted.

The **Information Officer** (Municipal Manager) is ultimately responsible for ensuring that the organisation meets its legal obligations. Addressing any personal information and protection from queries from journalists or media outlets.

Below follow key positions and their areas of responsibility:

Assistant Information Officers / Directors	ICT Manager	Deputy Information Officers / Information Owner	Human Resource Finance: Salaries
Encouragement of compliance with the conditions for the lawful processing of personal information	Ensuring all ICT assets used for processing personal information meet capable security standards.	Dealing with requests made to the municipality	Classifying personal information in line with the POPI Act and Regulations. Maintaining internal procedures to support the effective handling and security of personal information.
Dealing with requests made to the municipality	Performing regular checks and scans to ensure	Reviewing all personal information protection procedures and	Reviewing all personal information protection procedures and related policies, in line with an agreed

	security hardware and software is functioning optimally	related policies, in line with an agreed schedule and make recommendations to the Information Officer/ Director where applicable.	schedule.
Working with the Regulator in relation to investigations conducted pursuant to Chapter 6 in relation to the directorate under his/ her control	Evaluating any third-party services, the organisation is considering using to process personal information. For instance, cloud computing services.	Ensuring that all employees, consultants and others that report to the Information Officer/ Directors are made aware of and are instructed to comply with this and all other relevant policies	Arranging personal information protection training and advice for the people covered by this policy.
Approving any personal information protection statement attached to communications such as e-mails and letters.			
Addressing any personal information protection queries from journalists or media outlets.			

8. GENERAL STAFF GUIDELINES

- a) Access to any personal and confidential information are available to the parties who need the information to complete their duties.
- b) Personal information should not be shared informally and must never be shared over social media accounts such as Facebook, LinkedIn, Google Plus, etc.
- c) Training will be provided to all employees to understand their responsibilities when handling personal information.
- d) All personal information should be kept secure and not be disclosed to
- e) unauthorised individuals within the municipality or externally.
- f) Personal information must be reviewed regularly and updated. If no longer required, it should be deleted and disposed of in line with the disposal instructions within the Records Management Policy.
- g) If unsure about any aspect of the protection of personal information, the
- h) Assistant or Deputy Information Officers should be contacted.

9. QUALITY OF INFORMATION

A responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary. In taking the steps referred to the aforementioned the responsible party must have regard to the purpose for which personal information is collected or further processed.

10. DOCUMENTATION

A responsible party must maintain the documentation of all processing operations under its responsibility as referred to in section 14 of the Promotion of Access to Information Act.

11. COLLECTION OF PERSONAL INFORMATION

Information are collected to deliver a quality service to the public. Personal information is collected directly from data subjects where practical and should be in compliance with POPIA.

Personal information may be collected the following channels:

- a) Application forms for vacant positions;
- b) Tenders and Contracts;
- c) Websites;
- d) Through surveillance cameras (with facial recognition technology);
- e) Through third party service providers;
- f) Social media platforms;
- g) Responding to questionnaires;
- h) Surveys;
- i) Section 14 PAIA Requests

12. REASONS FOR KEEPING PERSONAL INFORMATION

The municipality may collect and process personal information for the following reasons:

- a) Employment and remuneration and other Human Resources needs
- b) Process benefits i.e. medical aid and pension
- c) Considering bids in terms of tenders and quotations;
- d) Closing agreements and contracts;
- e) Communication; sending and sharing of important information;
- f) Register services
- g) Maintaining Data base for essential services, indigent support, housing,
- h) Respond to inquiries; complaints and requests;
- i) Community consultation and feedback;
- j) Addressing the needs and priorities
- k) Understanding the needs and priorities of the community and other stakeholders;
- l) Security background checks (vetting)
- m) Rendering accounts
- o) Reports to council for bad debt
- p) Disclosure
- q) Audit reports

13. UTILISATION OF PERSONAL INFORMATION

Personal information will only be used for the intended purpose. Consent should be obtained from the data subject, if information is to be used for additional practises.

14. SHARING PERSONAL INFORMATION

The municipality shall only share personal information if the municipality has obtained consent in writing from the data subject.

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

- a) SARS
- b) Medical aids, Pension funds
- c) Financial institutions for remuneration purposes and payments
- d) In response to a request for information by a legitimate authority in accordance with, or required by any applicable law, regulation, or legal process;
- e) Where necessary to comply with judicial proceedings, court orders;
- f) To protect the rights, property, or safety of the municipality or others, or as otherwise required by an applicable law; and

15. THIRD PARTY INSURANCE

Service providers are contractually required to implement suitable information protection and security measures for any personal information that are shared by the municipality. Personal information will only be used for the intended purpose by the Third Party.

16. SAFEGUARDING OF PERSONAL INFORMATION

The municipality is committed to protect personal information from misuse, loss, theft, unauthorized access, modification, or disclosure

17. PUBLIC PARTICIPATION AND SERVICE DELIVERY COMMUNICATIONS

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.

18. DATA SUBJECTS: REQUEST TO ACCESS AND MANAGE PERSONAL INFORMATION

Data subjects have the right to request what personal information the municipality holds about them and why.

- a) The data subject may request the municipality to access, amend, 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.
- b) The data subject may withdraw or / and object to consent at any time for current or future processing
- c) The Municipality shall inform the data subject of an information breach.
- d) The data subject has the right to object to the processing of his / her personal information.
- e) The data subject has the right to submit a complaint to the Information Regulator regarding and alleged infringement of any of the rights protected under POPIA.

Access to information can be addressed to the Information Officer. The data subject will be provided with a Personal Information Request form. Once the completed form has been received the Information Officer will verify the identity of the data subject. The Information Officer will acknowledge receipt of any such request within three (3) days of the date of submission. 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. All requests will be processed and considered against the Section 14 Manual.

A responsible party may or must refuse, as the case may be, to disclose any information requested in terms of subsection (1) to which the grounds for refusal of access to records set out in the applicable sections of Chapter 4 of Part 2 and Chapter 4 of Part 3 of the Promotion of Access to Information Act apply. The provisions of sections 30 and 61 of the Promotion of Access to Information Act are applicable in respect of access to health or other records

19. POPIA COMPLAINTS PROCEDURE

Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. POPIA related complaints in accordance with the following procedure:

1. POPIA complaints must be submitted to the organisation in writing. Where so required, the Information Officer will provide the data subject with a "POPIA Complaint Form".
2. The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 3 working days.
3. 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.
4. 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.
5. 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 inform data subjects and the Information Regulator will of this breach.
6. 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 20 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.

20. BREACHES OF THE ACT OR POLICY

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

Disciplinary action and procedures in terms of the applicable code of conduct will be installed against the alleged perpetrator.

21. MUNICIPAL WEBSITE

The user have accepted the terms and conditions as specified on the Municipality's website. Other sites, via links can be accessed. These sites are not monitored, maintained or controlled by the municipality and thus we are not responsible in any way for any of their contents. The municipality are 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.

22. RETENTION OF PERSONAL INFORMATION

The West Coast DM shall retain personal information to comply with the prescriptions in the Records Management Policy and the Western Cape Provincial Archives and Records Service of the Western Cape Act, 2005 (Act no 3 of 2005) whereafter it will be disposed / transferred. Retention periods of documents containing personal data can vary.

23. 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.

24. MONITORING AND ENFORCEMENT

1. All employees will be responsible for administering and overseeing the implementation of this policy including the supporting of guidelines, standard operating procedure, notices, consents and appropriate related documents and processes.
2. Employees who violate the guidelines and standard operating procedures of this policy may be subjected to disciplinary action, being taken against him/her.
3. The point of contact for requests, disclosures, questions, complaints and any other inquiries relating to the processing, collection, or re-identifying of personal information shall be directed to the information officer or deputy information officer(s)

D. Signature Page
Signature
Date

D. Signature Page
Signature:
Date

INFORMATION OFFICER APPOINTMENT FORM

I herewith and with immediate effect appoint you as the Information Officer as required by the Protection of Personal Information Act (Act 4 of 2013). This appointment may at any time be withdrawn or amended in writing.

You are entrusted with the following responsibilities:

Taking steps to ensure the organisation's reasonable compliance with the provision of POPIA.

Keeping the governing body updated about the organisation's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations pursuant to popIA.

Continually analysing privacy regulations and aligning them with the organisation's personal information processing procedures. This will include reviewing the organisation's information protection procedures and related policies.

Ensuring that POPI Audits are scheduled and conducted on a regular basis,

Ensuring that the organisation makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to the organisation, to do so. For instance, maintaining a "contact us" facility on the organisation's website.

Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by the organisation. This will include overseeing the amendment of the organisation's employment contracts and other service level agreements.

Encouraging compliance with the conditions required for the lawful processing of personal information.

Ensuring that employees and other persons acting on behalf of the organisation are fully aware of the risks associated with the processing of personal information and that they remain informed about the organisation's security controls.

Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the organisation.

Addressing employees' POPIA related questions.

Addressing all POPIA related requests and complaints made by the organisation's data subjects.

Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

I hereby accept the appointment as Information Officer

Name and Surname

Signature

Date