Province of the
EASTERN CAPE
COOPERATIVE GOVERNANCE
& TRADITIONAL AFFAIRS

PROTECTION OF PERSONAL INFORMATION POLICY

2024

Departmental Contact Details	
Physical Address	Tyamzashe Building Phalo Avenue Bhisho 5605
Postal Address	Department of Cooperative Governance & Traditional Affairs Private Bag X0035 Bhisho 5605
Document Number	1
Document Name	Protection of Personal Information Policy
Contact Person	Mr M.P. Madikane
Designation	Director
Component	Employee Relations & Wellness
Telephone No.	040 940 7208
Cell Phone No.	082 521 3841
Fax No.	N/A
E-mail Address	mpumelelo.madikane@eccogta.gov.za
Date Completed	28 March 2024
Date of Approval	TBC
Date Last Amended	28 March 2024
Date For Next Review	March 2029
Related Policies	ICT Security Policy; Records Management Policy;

Executive Authority
Initials Z. A. W

AHOD
Initials_____

SIGN OFF

1. Head of Department

This Policy on the Protection of Personal Information has been recommended by Mr. V. Mlokothi in his capacity as Acting Head of Department for the Eastern Cape Department of Cooperative Governance and Traditional Affairs.

I am satisfied and concur with the contents of this Policy.

The development of the policy on POPIA will ensure the department is able exercise its powers in compliance with the law and guide decision- making in the department.

Recommended	
Designation	Acting Head of Department
Date	29/07/2024

2. Executive Authority

The Department of Cooperative Governance and Traditional Affairs has unprecedented opportunity to improve the lives of the staff by effectively rendering services that it is expected to provide. We have envisaged a department that has the required capacity to respond adequately to challenges of its staff.

I therefore trust that the guidance from Protection of Personal Information (POPIA) Policy will contribute to the effective management of Personal information in the Department.

Signed	
Designation	MEC: Honourable Mr. Z. Williams for the Eastern Cape Department of Cooperative Governance and Traditional Affairs
Date	05/08/2024

Executive Authority
Initials Z.A.W.

AHOD
Initials LG

TABLE OF CONTENTS

1. PREAMBLE

Parliament of the Republic of South African promulgated the Protection of Personal Information Act No.4 of 2013. The commencement date for section 1 dealing with definitions, Part A of Chapter 5 dealing with establishment of the Regulator, section 112 and 113 dealing with powers to make regulations and procedures thereof, commenced on 11 April 2014.
The rest of other sections, except for sections 110 and 114(4), commenced on 1 July 2020, with a further grace period ending on 30 June 2021.

The POPIA introduced minimum requirements for processing personal information and such requirements necessitate changes on how personal information is collected, used, stored and destroyed. The rights of data subjects are entrenched in the POPIA. The rights include consent to the processing of data subject's personal information, to request, where necessary, the correction, destruction or deletion of the personal information and to object to the unlawful usage of the personal information.

The policy is therefore intended to ensure compliance with POPIA by all staff in the department and observe the rights of data subjects.

2. PURPOSE OF POLICY

The purpose of this policy is to ensure that the Department handles the personal information at its disposal in a manner that does not undermine the constitutional right to privacy and as prescribed by the Protection of Personal Information Act 4 of 2013 and regulations.

3. POLICY OBJECTIVES

The objectives of this policy are: -

3.1 To promote and enhance compliance with conditions of lawful processing of personal information in the department.

3.2 To provide for internal measures for processing of personal information data in the department.

3.3 To stipulate the roles of responsible parties of the department when handling personal information.

3.4 To provide measures for reporting and handling personal information security compromises.

3.5 To promote and protect rights of data subjects by the department.

4. APPLICATION AND SCOPE

The provisions of this policy shall apply to all employees and decision makers involved in the handling of personal information in the department.

5. DEFINITIONS AND TERMS

WORD/TERM	DEFINITION
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 person to whom personal information relates.
Operator	means a person who processes personal information for the responsible party in terms of a contract or mandate, without coming under direct authority of that party.
Personal information	means information relating to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person, including, but not limited to- (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, 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, email address, physical address, telephone number, location information, online identifier or other assignment to the person; (d) the biometric information of that person; (e) the personal opinions, views or preferences of the person; (f) correspondence sent by the person that 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 that person.
POPIA	means Protection of Personal Information Act 4 of 2014
Processing	means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including- (a) the collection, receipt, recording, organisation, collation, storage, updating or modifications, re-trieval, 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 restriction, degradation, erasure or destruction of information.
Record	means any recorded information- (a) regardless of form or medium, including any of the following- (i) writing on any material; (ii) 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;

	(iii) label, marking or other writing that identifies or describes anything of which it forms part or to which it is attached by any means; (iv) book, map, plan, graph or drawing; (v) photograph, film, negative, tape or other device in which one or more visual images are embedded so as to be capable, with or without the aid of some other equipment, of being reproduced; (b) in the possession or under control of a responsible party; (c) whether or not it was created by a responsible party; and (d) regardless of when it came into existence.
Regulator	means the Information Regulator established in terms of section 29 of the Protection of Personal Information Act 4 of 2013.
Responsible party	means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

6. LEGAL FRAMEWORK

6.1 Constitution of the Republic of South Africa, 1996

6.2 Protection of Personal Information Act 4 of 2013

6.3 Promotion of Access to Information Act 2 of 2000

6.4 Public Service Act, 1994 (Proclamation 103 of 1994) and regulation

7. POLICY PRINCIPLES

7.1 Accountability

The department acknowledges that it is accountable to the data subjects by ensuring that their rights are respected and protected and that their personal information may not be processed in a manner that is inconsistent with the Constitution and legislation.

7.2 Confidentiality

The Departmental staff must, both during and after term of their employment in the department, treat as confidential the personal information which comes to their knowledge in the course of performance of their official duties, except if such information is required by law.

7.3 Respect for the Rule of Law

The department acknowledges its Constitutional obligation as an organ of State to only exercise public power if it is authorised by law to do so. In so far as it relates to personal information at its disposal, the department undertakes to respect the Constitutional right to privacy and observe the lawful conditions for processing of personal information.

8. POLICY STATEMENT

The department, in pursuing its mandate, processes Personal Information of its employees, its stakeholders and / or clients such as potential service providers, service providers and individual members of the community and corporate entities.
The department therefore regards the lawful processing and usage of all Personal Information of data subjects as essential in maintaining confidence between it and its stakeholders and for successful execution of its mandate.

9. DATA COLLECTION BY THE DEPARTMENT

When collecting Personal Information from a Data Subject, Responsible Parties must –

9.1 ensure that they obtain the informed consent of the Data Subject to process the Personal Information of the concerned Data Subject, including, but not limited to, informing the Data Subject of the potential use of their Personal Information, where the Personal Information might be processed and/or stored, as well as the notification procedures that will be used to inform the Data Subject of changes to the scope of the use of their Personal Information and/or any security breaches that might relate to their Personal Information; and

9.2 inform the Data Subject about his/her rights under the provisions of POPIA, including the Data Subject's right to –

9.2.1 object to the Processing of their Personal Information;

9.2.2 notification(s) if their Personal Information is being used for purposes other than what they consented to the Personal Informing being collected and used for;

9.2.3 establish whether the Responsible Party holds their Personal Information;

9.2.4 request that their Personal Information held by the department be corrected or destroyed;

9.2.5 refuse the processing of their Personal Information for direct marketing purposes, such as unsolicited electronic communications;

9.2.6 lodge a complaint with the information regulator, as constituted in terms of POPIA and any regulations thereto, against the Responsible Party;

10. PROCESSING PERSONAL INFORMATION

The following conditions for the lawful processing of personal information must be complied with when personal information is processed within the department.

10.1 Accountability.

The responsible parties must ensure that the conditions set out in POPIA are complied with at the time of the determination of the purpose and means of Processing as well as during Processing itself.

10.2 Purpose Specification.

The personal information collected from the Data Subject must be collected for a specific purpose and the Data Subject must be made aware of this purpose.

10.3 Processing Limitations.

The following processing limitations apply, namely –

10.3.1 The Data Subject must consent to the processing of their Personal Information;

10.3.2 Only the minimal amount of Personal Information needed in order to complete the Processing purpose and/or its requirements is obtained from the Data Subject;

10.3.3 The Data Subject must be informed of their rights as stipulated in paragraph 9.2 of this Policy and any other rights lawfully granted to the Data Subject;

10.3.4 All Personal Information must be collected directly from the Data Subject, except to the degree that the Data Subject consents otherwise; and

10.3.5 All Personal Information must be processed lawfully and in accordance with the law.

10.4 Further Processing Limitation.

The renewed consent of the Data Subject must be obtained if the personal information of the Data Subject will be processed for a further purpose and/or different purposes, unless the further processing of the Data Subject's personal information is reasonably related to the same purpose it was initially collected for from the Data Subject

10.5 Information Quality.

Reasonable measures must be taken to ensure that the personal information collected from the Data Subject is complete, accurate, not misleading and is up to date. Employees are obliged to ensure that at all times they provide the department with complete, accurate, and up to date personal information;

10.6 Openness.

The purpose of the collection of the Data Subject's personal information must be transparent. The Data Subject must be reasonably made aware of their rights (as stipulated in paragraph 9.2

of this Policy) and what measures the Data Subject can take to have their Personal Information adapted or deleted, if the Data Subject in question requests this of the Responsible Party.

10.7 Security Safeguards.

Personal Information collected from a Data Subject must be securely kept (in accordance with the requirements stipulated in section 11 of this Policy). The integrity of all Personal Information must be maintained through all technical and organisational measures and/or processes.

10.8 Data Subject Participation.

The Data Subject has the right to request and to find out whether the Responsible Party and/or Department holds their Personal Information and a description of the Personal Information held by the Responsible Party.

11. STORAGE OF PERSONAL INFORMATION

11.1 HARD COPIES

11.1.1 All hard copies of Personal Information must be stored at the registries of the department and in a manner prescribed by departmental records management policy.

11.1.2 Any hard copies must be retained for as long as the Personal Information is in use and for a period prescribed by the departmental records management policy, unless otherwise agreed with the Data Subject at the date of the collection of the Data Subject's Personal Information.

11.2 ELECTRONIC COPIES

11.2.1 The Departmental records management system must have reasonable technical and organisational measures to prevent loss of, damage to, or unauthorised destruction of any Personal Information; and the unlawful access to, or processing of Personal Information.

11.2.2 In order to give effect to the provisions of clause 11.2.1, the department must take reasonable measures to:

11.2.2.1 identify all reasonably foreseeable internal and external risks to Personal Information in its possession or under its control;

11.2.2.2 establish and maintain appropriate safeguards against the risks identified;

11.2.2.3 regularly verify that the safeguards are effectively implemented; and

11.2.2.4 ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

12. DESTRUCTION OF PERSONAL INFORMATION

12.1 Personal Information must be destroyed or deleted once they are no longer needed or in use and after the termination of the retention period(s) permitted in the departmental records management policy.

12.2 The Responsible Parties are responsible for attending to the destruction or deletion of Personal Information or any related documentation held by it on a regular basis. Personal Information must be checked before its destruction or deletion to ascertain if the information may be destroyed or deleted and whether there are any important original documents that may be returned to the Data Subject.

13. HANDLING OF SECURITY COMPROMISES

13.1 Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the Information Officer should be contacted immediately.

13.2 The Information Officer is required to notify the information regulator and the data subject.

13.3 The notification of a breach of confidentiality should be declared as soon as is reasonably possible upon the discovery of the compromise.

13.4 The Information Officer needs to provide sufficient information to the data subject which will enable the data subject to take protective measures against the potential consequences of the compromise.

14. MEASURES TO PROTECT PERSONAL INFORMATION IN THE DEPARTMENT

In order to protect personal information, the following must be done:

14.1 Internal awareness sessions regarding the provisions of the POPIA and its regulations, codes of conduct or information obtained from the regulator, must be conducted.

14.3 Employees must be trained on this policy and POPIA.

14.3 Each new employee will be required to sign an employment contract that contains relevant consent and confidentiality clauses for the use and storage of personal information, in terms of POPIA.

14.4 Every employee currently employed within the Department will be required to sign an addendum to their employment contract, containing relevant consent and confidentiality clauses for the use and storage of personal information, in terms of POPIA.

14.5 Ensuring that personal information is encrypted prior to sharing the information electronically.

14.6 Ensuring that all devices such as computers, flash drives, etc. are password protected and never left unattended (refer to the departmental ICT Security policy).

14.7 Ensure that computer screens and other devices are switched off when not in use.

14.8 Ensure that removable storage devices such as external drives that contain personal information are locked away securely when not being used.

14.9 Ensure that where personal information is stored on paper and that such hard copies are kept in a secure place where unauthorised persons are not able to access it.

14.10 Ensure that where personal information has been printed out, that the printouts are not left unattended where unauthorised individuals could see them.

14.11 Take reasonable steps to ensure that personal information is stored only for as long as it is needed or required.

15. ROLES AND RESPONSIBILITIES

15.1 Head of Department (Information Officer)

15.1.1 Ensuring that the Department makes it convenient for Data subjects to communicate with the Department regarding their personal information.

15.1.2 Encourage compliance with the lawful processing of personal information.

15.1.3 Address employees' POPIA related questions.

15.1.4 Address POPIA related requests and complaints made by the Department's Data subjects; and

15.1.5 Act as contact point for the Information Regulator on issues pertaining to the processing of personal information.

15.1.6 To designate an official to drive the implementation of POPIA in the department.

15.2 Management and staff

15.2.1 Must comply with conditions for the lawful processing of personal information set out in chapter 3 of POPIA and clause 10 of this policy when personal information is processed within the department.

15.2.2 Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, to notify the data

subject and Information Officer for referral to the Regulator. In appropriate circumstances notifications can be referred directly to the Regulator.

15.2.3 Must secure the integrity and confidentiality of personal information in their possession or control.

15.2.4 Must take appropriate and reasonable measures to prevent the loss or damage to, or unauthorised destruction of, personal information and unlawful access to, or processing of, personal information.

15.2.4 Must have due regard to generally accepted information security practices and procedures which may apply generally or be required in terms of legal framework applicable in the public service. Such practices may include but not limited to:

15.2.4.1 Applying a clean desk policy

15.2.4.2 Storing hard copies in filing cabinets that can be locked

15.2.4.3 Check recipient before sending an email.

15.3 Records Manager

15.3.1 Develop measures to ensure that personal information at the disposal of the department is stored in a manner that does compromise its security.

15.3.2 Develop measures regarding retention period of personal information as may be prescribed by the records management policy of the department.

15.3.3 Develop measures to regulate destruction of personal information in accordance with this policy and /or records management policy and POPIA.

15.3.4 Ensure that a manual is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);

15.3.5 Ensure that internal measures are developed together with adequate systems to process requests for information or access thereto.

15.4 Director: Departmental Government Information Technology Office (DGITO)

15.4.1 Develop measures to ensure that the Department's IT infrastructure and any other devices used for processing personal information meet acceptable security standards;

15.4.2 Develop measures to ensure that servers containing personal information are sited in a secure location;

15.4.3 Develop measures to ensure that all electronically stored information is backed-up and tested on a regular basis;

15.4.4 Ensures that all back-ups are protected from unauthorised access, accidental deletion and malicious hacking attempts;

15.4.5 Develop measures to ensure that information being transferred electronically is encrypted;

15.4.6 Ensures that all servers and computers containing personal information are protected by a firewall and the latest security software;

15.4.7 Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by unauthorised persons.

15.5 Designated official

15.5.1 To facilitate institutionalisation of the POPIA in the department working with all other role players;

15.5.2 In collaboration with Legal Advisory Services, organize regular internal awareness sessions regarding the provisions of the POPIA and its regulations, codes of conduct or information obtained from the regulator,

15.5.3 Coordinate development, implementation and monitoring of POPIA compliance framework;

15.5.4 Facilitate personal information impact assessment to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;

15.5.5 In collaboration with Human Resource Utilisation and Capacity Building, facilitate training of employees on this policy and POPIA;

15.5.5 In collaboration with all role players involved in processing of personal information in the department and guided by Risk Management, to facilitate identification and

monitoring of risks associated with processing of personal information in the department.

16. MONITORING AND REPORTING

The designated official will monitor implementation of this policy and provide quarterly reports to the Head of Department.

17. COMMITMENT AND CONSEQUENCES OF NON-COMPLIANCE

17.1 POPIA implementation in the department is the responsibility of all staff and management and thus require a collective and collaborative effort.

17.2 Commitment by management and staff is imperative because consequences of non-compliance may result in a serious reputational damage and severe penalties by the Information regulator.

17.3 The department must therefore capacitate staff and management on POPIA.

17.4 Where there is non-compliance with the requirements of this policy, disciplinary action shall be considered in accordance with the applicable disciplinary code.

18. COMMUNICATION OF THE POLICY

The Protection of Personal Information Policy must be communicated to all staff members by placing it in the intranet, issuing circulars and ongoing advocacy sessions

19. REVIEW OF THE POLICY

The policy must be reviewed every five years or as and when there are developments in POPIA and its regulations, guidelines and codes of conduct issued by the Regulator.

20. DATE OF EFFECT AND APPROVAL

Protection of Personal Information Policy will become effective upon approval by the Executive Authority.

21. VERSION CONTROL AND CHANGE HISTORY

Version Control	Date Effective	Approved By	Amendment
	30/07/2024		Z.A. Williams.

Executive Authority Initials Z.A.W

AHOD Initials