



Province of the
EASTERN CAPE
COOPERATIVE GOVERNANCE
& TRADITIONAL AFFAIRS

RETENTION OF PERSONAL INFORMATION POLICY 2025

RETENTION OF PERSONAL INFORMATION POLICY 2025

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	Retention of Personal Information Policy
Contact Person	Mr SB Maqungo
Designation	Director
Component	Legal Services
Telephone No.	040 940 7119
Fax No.	N/A
E-mail Address	siphiwo.maqungo@eccogta.gov.za
Date Completed	
Date of Approval	
Date For Next Review	2029
Related Policies	Protection of Personal Information Policy;

RETENTION OF PERSONAL INFORMATION POLICY 2025

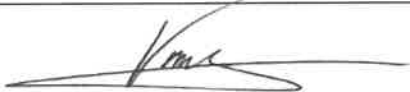
SIGN OFF

1. Head of Department

This Policy on the Retention of Personal Information has been recommended by Mr. V. Mlokothe in his capacity as 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 this policy will ensure that the department comply with the provisions of section 14 of the Protection of Personal Information Act, 2013.

Recommended	
Designation	Head of Department
Date	24th December 2025

2. Executive Authority

The Department of Cooperative Governance and Traditional Affairs, as an organ of state and to which the Protection of Personal Information Act, 2013 applies, may not retain the records of personal information for longer than is necessary to achieve the purpose for which it was collected.

I therefore trust that the guidance from Retention of Personal Information Policy will contribute to the effective management of Personal information as it relates to retention periods in the Department.

Signed	
Designation	MEC: Honourable Mr. Z. A. Williams for the Eastern Cape Department of Cooperative Governance and Traditional Affairs
Date	21 - 01 - 2026

RETENTION OF PERSONAL INFORMATION POLICY 2025

TABLE OF CONTENTS

<u>CONTENT</u>	<u>PAGE(S)</u>
1. Purpose	4
2. Policy Objectives	4
3. Application, scope and interpretation	4
4. Definitions	5
5. Legal Framework	6
6. Policy Principles	6
7. Retention rules	7
8. Destroying and de-identifying data	8
9. Breach, enforcement, and compliance	9
10. Record disposal	9
11. Retention register	10
12. Monitoring and reporting	10
13. Communication of the policy	10
14. Review of the policy	10
15. Date of effect and approval	10
16. Version Control and Change History	10

RETENTION OF PERSONAL INFORMATION POLICY 2025

1. PURPOSE

The purpose of this policy is to set out the required retention periods for specified categories of information, including personal information, and to establish minimum standards to be applied when destroying certain personal information within the organisation.

2. POLICY OBJECTIVES

The objectives of this policy are: -

- 2.1 To promote the protection of personal information that is in custody of the department by ensuring that its retention is not longer than is necessary for achieving the purpose for which it was collected or subsequently processed.
- 2.2 To minimise the risk of breach of personal information security by prescribing the retention periods and the manner of destroying personal information that is no longer required.

3. APPLICATION, SCOPE AND INTERPRETATION

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

- 3.1 All appointed contractors, consultants, advisors, or service providers of the department that may collect, process, or have access to information (including personal information).
- 3.2 All data/information held by the department, including personal information as defined in the Protection of Personal Information Act (“POPIA”), irrespective of the format it is held including but not limited to, electronic information, electronic mail, hard copy documents, digitally recorded information such as voice recordings, photographs and video footage, CCTV footage, information generated by access control systems, COVID screening, etc.
- 3.3 The provisions of this policy are subject to the departmental Records Management Policy.

RETENTION OF PERSONAL INFORMATION POLICY 2025

4. DEFINITIONS

The terms listed hereunder shall bear the following meanings:

4.1 ‘Data’ means all information in possession or under the control of the organisation, irrespective of the nature thereof.

4.2 “De-identify” means in relation to personal information of a data subject, means to delete any information that—

- (a) identifies the data subject;
- (b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
- (c) can be linked by a reasonably foreseeable method to other information that identifies the data subject.

4.4 Deputy Information Officer means the person designated as such by the Information Officer in terms of section 17 of Promotion of Access to Information Act 2 of 2000.

4.5 Information Officer as defined in by section 1 of the Promotion of Access to Information Act 2 of 2000, is the Head of Department.

4.3 “PAIA” means the Promotion of Access to Information Act 2 of 2000.

4.4 “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, 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, e-mail address, physical address, telephone number, location information, online identifier, or other particular assignment to the person.

RETENTION OF PERSONAL INFORMATION POLICY 2025

- (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.

4.5 “Personal information of children” means personal information about a natural person under the age of 18 years as referred to in section 34 of POPIA

4.6 “POPIA” means the Protection of Personal Information Act, 4 of 2013.

4.7 “Special Personal Information” means personal information as referred to in section 26 of POPIA; and

4.8 “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 devices, 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 another device in which one or more visual images are embodied to be capable, with or without the aid of some other equipment, of being reproduced.

(b) in the possession or under the 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.

5. LEGAL FRAMEWORK

RETENTION OF PERSONAL INFORMATION POLICY 2025

5.1 Constitution of the Republic of South Africa, 1996

5.2 Protection of Personal Information Act 4 of 2013

5.3 Promotion of Access to Information Act 2 of 2000

5.4 Public Service Act, 1994 (Proclamation 103 of 1994) and regulations

6. POLICY PRINCIPLES

6.1 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 retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed unless the retention is required by law.

6.2 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.

6.3 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 undertake to respect the Constitutional right to privacy and observe the lawful conditions for processing of personal information.

7 RETENTION RULES

7.1 General Principles

7.1.1 Information must be held in terms of statutory retention periods and may be held in the legitimate interest of the department.

RETENTION OF PERSONAL INFORMATION POLICY 2025

- 7.1.2 It is the responsibility of the Information Officer to determine retention periods, in consultation with relevant staff members, in respect of information that is held otherwise than in terms of statutory retention periods.
- 7.1.3 In the event any category of records is not specified in this policy (and in particular within the Data Retention Schedule) and unless otherwise mandated by applicable law, the required retention period for such record will be determined by the Information Officer on request, taking into consideration the principles set out in POPIA.

7.2 Retention Periods

- 7.2.1 The Information Officer defines the period for which records should be retained as set out in the Data Retention Schedule.
- 7.2.3 As an exemption, retention periods within the Data Retention Schedule can be extended within the discretion of the Information Officer, within the requirements of POPIA, where special circumstances justifiable in terms of POPIA or PAIA exist, which may include protection against potential litigation, pending litigation, request by or consent of the data subject, etc.

8. DESTROYING AND DE-IDENTIFYING DATA

- 8.1 The department and its employees should, on a regular basis, review all data and parts thereof in terms of this policy, irrespective of the format thereof and where it is stored, to determine whether the data should be retained, de-identified, destroyed or deleted, either because of the expiry of the retention period or if the reason for which it was collected or retained is no longer relevant.
- 8.2 The ultimate control and responsibility for the destruction of data is the responsibility of the Information Officer.
- 8.3 If a decision is made to retain records for historical, research or statistical purposes, the information should be de-identified.
- 8.4 Once the decision is made to destroy or delete data in accordance with this Guideline and the Retention Schedule, the data should be deleted, shredded or otherwise destroyed to a degree equivalent to their value to others and their level of confidentiality. The method of disposal may vary and is dependent upon the nature of the record. For example, any records that contain

RETENTION OF PERSONAL INFORMATION POLICY 2025

sensitive or confidential information (and particularly personal information) shall be disposed of as confidential waste and be subject to secure electronic deletion. The Record Disposal Schedule section below defines the mode of disposal.

- 8.5 In this context, employees delegated for this purpose by the Information Officer shall perform the tasks and assume the responsibilities relevant for the information destruction in an appropriate way.

The specific deletion or destruction process may be carried out either by an employee or by an internal or external service provider that the Information Officer subcontracts for this purpose. Any applicable general provisions under relevant data protection laws and the departmental Privacy Policy shall be complied with.

The Information Officer shall fully document and approve the destruction process.

9. BREACH, ENFORCEMENT AND COMPLIANCE

- 9.1 It is the responsibility of the Information Officer to ensure that the entire organisation complies with these imperatives.

- 9.2 Any suspicion of a breach of this rule must be reported to the Information Officer immediately. All instances of suspected breaches of this rule shall be investigated and appropriate action taken.

- 9.3 Failure to comply with this rule may result in serious adverse consequences, including, but not limited to, loss of client confidence, litigation, financial loss, administrative fines imposed by the Regulator and damage to the organization's reputation, personal injury, harm or loss. Non-compliance with this policy by employees or any third parties who have been granted access to departmental premises or information, may therefore result in disciplinary proceedings in appropriate circumstances in respect of employees or to the termination of the contract in appropriate circumstances in respect of third parties. Non-compliance may also lead to legal action against the parties involved in such activities.

10. RECORD DISPOSAL

10.1 Destruction Method

- 10.1.1 Level I records are those that contain information that is at the highest security and confidentiality level and those that include any personal information. These records shall be

RETENTION OF PERSONAL INFORMATION POLICY 2025

disposed of in a manner that the data is destroyed and cannot be reconstructed. Disposal of the records must include proof of destruction.

10.1.2 Level II records are proprietary records that contain confidential information such as parties' names, signatures, and addresses, or which could be used by third parties to commit fraud, but which do not contain any personal information. The records shall be disposed of in the manner that the data is entirely destroyed and cannot be reconstituted. Disposal of the records must include proof of destruction.

10.1.3 Level III records are those that do not contain any confidential information or personal information such as organisation records in the public domain. These may be shredded and disposed of through recycling. Disposal of the records does not need proof of destruction.

11. RETENTION REGISTER

11.1 EC COGTA Retention period is 5 years unless otherwise advised by internal needs.

12. MONITORING AND REPORTING

12.1. The Information Officer and /or Deputy Information Officer will monitor implementation of this policy and provide reports as may be required by relevant bodies, including but not limited to, the Audit Committee, Office of the Premier and the Information Regulator.

13. COMMUNICATION OF THE POLICY

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

14. REVIEW OF THE POLICY

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

15. DATE OF EFFECT AND APPROVAL

RETENTION OF PERSONAL INFORMATION POLICY 2025

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

16. VERSION CONTROL AND CHANGE HISTORY

Version Control	Date Effective	Approved By	Amendment