Province of the
EASTERN CAPE
SOCIAL DEVELOPMENT

Privacy Policy

Department of Social Development

Policy Registration 2026-04

Table of Contents

Legislative Frameworks

1. Constitution of the Republic of South Africa, 1996
2. Public Finance Management Act (Act No.1 of 1999)
3. National Archives and Record Service Act (Act No. 43 of 1996)
4. Protection of Personal Information Act (Act No. 4 of 2013)
5. The Cybercrimes Act (Act No. 19 of 2020)
6. Electronic Communications and Transactions Act (Act No. 25 of 2002)
7. Promotion of Access to Information Act (Act No. 2 of 2000)
8. Promotion of Administrative Justice Act (Act No. 3 of 2000)
9. Minimum Information Security Standard (1996)
10. State Information Technology Act (Act No. 88 of 1998)
11. Labour Relations Act (Act No. 66 of 1995)
12. Control of Access to Public Premises Act (Act No. 53 of 1985)
13. Treasury Regulations, 2005
14. National Development Plan 2030
15. Public Service Regulations, 2016

Terms and Definitions

Terms	Definitions
Administration	Administration is the process of managing user identities, roles, and credentials they are assigned, and the resources and services they use.
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.
Child	A child means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him or herself
Consent	Means any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of personal information
Cookies	Small text files placed on a device to store data that can be recalled by a web server in the domain that placed the cookie.
Database	A structured set of data held in a computer, especially one that is accessible in various ways, ranging from simple desktop systems to complex, multi-machine implementations.
Data Subject	This refers to the natural or juristic person to whom personal information relates, such as an individual client, customer or a company that supplies Department of Social Development with services, products, or other goods.
De-Identify	Refers to the deletion of any information that: (a) identifies the data subject, (b) can be used or manipulated by a reasonably foreseeable method to identify the data subject, and (c) can be linked by a reasonably foreseeable method to other information that identifies the data subject.
Direct Marketing	Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject, or requesting the data subject to donate any kind for any reason.
Electronic Communications	Any transfer of signs, signals, writing, images, sounds, or data transmitted via systems such as email, intranet, internet, and telephony.
End User	An official or authorised individual who utilises the information, computer equipment, and systems of the Department to perform their duties.
Executive Management	The highest level of leadership (e.g., CEO, CFO, COO) responsible for defining organisational strategy, setting long-term goals, and making high-stakes institutional decisions.
Filing System	Means any structured set of personal information, whether centralised, decentralised, or dispersed on a functional or geographical basis, which is accessible according to specific criteria.
Head of Department	The Accounting Officer of the Eastern Cape Department of Social Development, as defined by the Public Finance Management Act.
Host	A physical server that houses several virtual servers within it.
HTTP	Short for 'Hypertext Transfer Protocol'; the underlying protocol used by the World Wide Web which defines how messages are formatted and transmitted, and what actions web servers and browsers should take in response to various commands.

Information Assets	Valuable, identifiable data, systems, or information-related resources that an organization needs to operate, make decisions, and create competitive advantage. These include tangible items like servers and paper records, as well as intangible data like customer databases, software, and intellectual property.
Information Officer	The individual responsible for ensuring the Department of Social Development's compliance with POPIA. Where no Information Officer is appointed, the Head of Department shall be responsible.
Internet Protocol Address	A numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves two main functions: host or network interface identification and location addressing.
Member of Executive the Councillor	The Executive Authority appointed by the Premier to provide political leadership and oversight to the Provincial Department.
Personal Information	Information relating to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person, including but not limited to identifiers (name, ID, email, physical address); demographic data (race, gender, age); medical, financial, criminal, or employment history; biometric information; and personal opinions or private correspondence.
Privacy	Privacy refers to the right to protection against the unlawful collection, retention, dissemination, and use of personal information.
Processing	Any activity or set of operations, whether by automatic means, concerning personal information, including collection, receipt, recording, storage, modification, retrieval, dissemination, or destruction.
Operator	A person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party (e.g., a third-party service provider contracted to shred documents).
Record	Any recorded information, regardless of form or medium, including writing, electronic data, labels, maps, plans, or photographs, in the possession or under the control of the responsible party.
Responsible Party	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 Department of Social Development.
Restriction	To withhold from circulation, use, or publication any personal information that forms part of a filing system, but not to delete or destroy such information.
Third Party	A person who is sponsored or contracted by the Department and requires access to its resources.
Unique Identifier	Any identifier assigned to a data subject and used by a responsible party for the operations of that party, which uniquely identifies that data subject in relation to that party.
Special Personal Information	Highly sensitive data covered in Section 26-33 of POPIA, the processing of which is generally prohibited unless strict exemptions apply. This includes religious/philosophical beliefs, race, ethnic origin, trade union membership, political persuasion, health or sex life, biometric data, and criminal behaviour related to alleged offenses.
Acronyms	
CIO	Chief Information Officer
ECDSD	Eastern Cape Department of Social Development
GIF	Graphics Interchange Format
GITO	Government Information Technology Officer
ICT	Information and Communication Technology

IOS	iPhone Operating System/Internetwork Operating System
ISP	Internet Service Provider
IT	Information Technology
POPIA	Protection of Personal Information Act (No. 4 of 2013)

1. Preamble

The Department processes personal information in the course of its business activities. It uses this information to provide products or services, carry out requested transactions, and maintain relationships with clients, employees, and relevant stakeholders. 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 (No. 4 of 2013) (POPIA). Therefore, the Department respects individual privacy and takes the protection of personal information very seriously.

The Department provides social protection services and leads government efforts to forge partnerships through which vulnerable individuals, groups and communities become capable and self-reliant participants. A User's right to privacy entails having control over personal information and being able to conduct affairs relatively free from unwanted intrusions. This policy is committed to effectively managing personal information in accordance with POPIA provisions.

2. Purpose

The Privacy Policy informs departmental processes on the handling of personal information to foster trust and to ensure the protection of the privacy of beneficiaries, clients, customers, employees, and other stakeholders in line with legislative requirements.

3. Objectives

a) To mitigate the legal liability of the Department.
b) To provide assurance to clients and relevant stakeholders.
c) To protect the personal information of users.
d) To comply with all relevant regulatory and legislative frameworks.

4. Scope of Applicability

This policy is applicable to all the employees, contract workers, organisation contracted with the Department and individuals granted access to departmental systems.

5. Principles and Values

a) **Confidentiality**: means ensuring that information is only seen by people who have the right to see it.
b) **Integrity**: means ensuring that information remains intact and unaltered.
c) **Availability**: implies ensuring data subjects have access to their personal information when they need it.
d) **Accountability**: means accepting responsibility for actions and behaviour.
e) **Fairness and lawfulness**: when processing personal information, the individual rights of the data subjects must be protected. Personal information must be collected and processed in a legal and fair manner.
f) **Transparency**: the data subject must be informed of how their personal information is handled.

6. Policy Provisions

6.1. General Guiding Principles

Employees, contract workers and individuals granted access on behalf of the Department shall be subject to the following guiding principles:

6.1.1. Accountability

a) All the Departmental employees and other stakeholder must be accountable with their processes of processing personal information at the planning stage up to the disposal stage.
b) The Department shall take appropriate sanctions that include disciplinary actions against users failing to comply.

6.1.2. Processing Limitation

a) The Department ensures personal information under its control is processed fairly and lawfully.
b) The Department informs the data subject of reasons for collecting personal information and obtains written consent.
c) Department maintains a voice recording of the purpose for collecting personal information, obtaining consent for transactions concluded telephonically.
d) The data subject is informed of the possibility of sharing personal information with third parties.

6.1.3. Purpose Specification

a) Departmental business units and operations shall be informed about the principle of transparency.
b) Department processes personal information for specific, explicitly defined, and legitimate reasons.
c) Department shall inform data subjects of the reasons prior collecting or recording the data subject's personal information.

6.1.4. Further Processing Limitation

a) Personal information is processed for secondary purpose unless the processing is compatible with the original purpose.
b) The Department shall seek the consent from the data subject to process personal information for secondary purpose.

6.1.5. Information Quality

The Department has a duty in terms of the Protection of Personal Information Act (Act No. 4 of 2013) (**POPIA**) to ensure that it takes reasonably practicable steps to ensure that the personal information it collects and processes is complete, accurate, not misleading and updated where necessary. Accordingly, the Department shall:

a) Implement quality assurance systems guided by checklists when collecting information.
b) Update its records, through the User Access Review Form, by way of annually reviews.
c) Updates its records on an as and when basis (i.e., when the need arises).
d) Individuals also can update their own information on various other systems.

Data subjects shall be responsible for providing correct personal information and for informing the Department when the personal information they have provided needs to be updated.

6.1.6. Open Communication

a) The Department shall take reasonable steps to ensure data subjects are notified when their personal information is collected.
b) The Department shall ensure the establishment and maintenance of a 'contact us' facility for data subjects enquiring about their personal information.

6.1.7. Security Safeguards

a) Access to the personal information shall be based on roles and responsibilities.
b) The Departmental security policies, ICT security policies, Records Management Policy and other access procedures shall be used as the guides for the protection of personal information.
c) Personal information shall not be stored for longer than is necessary for the purposes described in this Privacy Policy or as required by applicable legislation.
d) The retention and disposal of personal information shall be guided by the Records Management Policy and shall be done in line with relevant legislation.
e) Investigating and reacting to security breaches, unlawful access, and other security incidents.
f) The Personal Information we collect from users shall only be accessed by our employees, representatives, and consultants on a need-to-know basis, and subject to reasonable confidentiality obligations binding such persons.

6.1.8. Data Subject Participation

POPIA provides for the protection of personal information. In conjunction, PAIA provides for the granting of access to information. The provisions covered in both Acts recognise numerous rights that data subjects can exercise in relation to the personal information the Department processes. Consequently, data subjects have the right to:

a) Request the Department to confirm, free of charge, whether it holds certain personal information about them.
b) Access a copy or record of the personal information the Department holds, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information.
c) Correct inaccurate personal information that the Department holds about them.
d) Restrict the Department's use of a data subject's personal information.
e) Ask the Department to destroy or delete the information it holds about them.
f) Object to the Department's use of their personal information.

6.2. Legal Basis for Processing Personal Information

The Department shall have a legal basis for processing the personal information of an employee, client, and or any other stakeholder. The following shall apply:

a) **Consent:** This shall be an explicit agreement granting the Department the right to process personal information for a specific purpose.

b) **Legitimate Interests:** This shall entail processing of personal information that is necessary for the Department to fulfil its mandate and perform its functions.

c) **Performance of a Contract:** This shall entail the processing of personal information to be able to fulfil a contractual obligation that the Department has with the data subject (e.g., employment contract).

d) **Legal Obligation:** This shall be any legal requirement to process personal information (e.g., Labour Relations Act).

6.2.1. Personal Data Processed by the Department

a) Clients and Partner Personal Information

i. Personal information processing for a contractual relationship; service access, and partnership on service delivery provision.
ii. Personal information processing for advertising purposes, for example to find parents, family members, invite bids and partners such NPOs.

b) Employee Personal Information

Personal information processing for the employment relationship; In employment relationships, personal data can be processed if needed to initiate, carry out and terminate the employment agreement. When initiating an employment relationship, the applicants' personal data can be processed. If the candidate is rejected, his/her information must be deleted in observance of the required retention period, unless the applicant has agreed to remain on file for a future selection process.

c) See Annexure A for personal data and special personal data processed by the Department.

6.2.2. Departmental Uses of Personal Information and Data

The Department shall use personal information in the following ways:

a) **Staff Administration**: To perform its functions as an employer (e.g., HR administration and Finance administration).

b) **Contact**: To be able to contact its employees, contractors, and clients.

c) **Reporting Requirements/Legislative Compliance:** To be able to respond to requests from the Auditor General of South Africa and the Department of Employment and Labour.

6.2.3. Processing of the Personal Information of Children

The Department shall process the personal information of children if one or more of the following applies:

a) Parent or guardian has consented.
b) The processing is needed to create, use, or protect a right or obligation in established in legislation.
c) The child's personal information is made public by the child with the consent of a parent or guardian.
d) The processing is for statistical, or research purposes and legal conditions are met.
e) The Department mandates a privacy impact assessment for systems handling children's data.

6.2.4. Interdepartmental Sharing of Personal Information

The following shall be entities with which, and circumstances in which the Department shares personal information in accordance with applicable legislation, national policies, and frameworks.

a) The Department of Employment and Labour.
b) The Government Employees Pension Fund (GEPF).
c) The Department of Treasury.
d) The Auditor General of South Africa.
e) Emergency services.
f) Contracted service providers.
g) Internally between the various directorates of the Department where necessary to perform its functions, including departmental entities such as the South African Social Security Agency (SASSA) and the National Development Agency (NDA).
h) Under legal obligation to law enforcement agencies, regulatory organisations, courts, or other public entities.
i) With any entity or forum wherein, the Department shall exercise or defend its rights to protect itself and the public interest.
j) If the Department is reorganised or amalgamated with another department and must transfer any personal information, it holds to the entity it is merging with.

6.2.5. Conditions for the Transfer of the Personal Information of a Data Subject

The Department shall only transfer personal information of the data subject to third parties in another country in one or more of the following circumstances:

a) Where the data subject's personal information shall be adequately protected under the other country's laws or an agreement with the third-party recipient.
b) Where the transfer is necessary to enter, or perform, under a contract with the data subject or a contract with a third party that is in the data subject's interest.
c) Where the data subject has consented to the transfer.
d) Where it is not reasonably practical to obtain the data subject's consent, but the transfer is in the data subject's interest.
e) The transfer shall happen only within the requirements and safeguards of applicable laws or privacy rules that bind the Department of Social Development.
f) Where possible the party processing a data subject's personal information shall be required to agree to apply the same level of protection of such personal information as is legally available in the data subject's country, and if the other country's laws provide better protection, the other country's laws shall be agreed to and applied.

6.2.6. Data Retention

The Department shall:

a) Keep different types of records in accordance with the Records Management Policy and as required by relevant legislation.
b) Retain relevant information in accordance with retention periods.
c) Store personal information in accordance with its use requirements as described in this Privacy Policy and as required by applicable legislation.
d) Dispose personal information as prescribed in the Records Management Policy and in line with applicable legislation.
e) Treat collected personal data and supporting documentation confidentially.

6.2.7. Notification of a Data Breach

a) In the event of a data breach leading to the accidental or unlawful damage, loss, modification, unauthorised disclosure, or any unauthorised access to a data subject's personal information that has been transmitted, stored, or otherwise processed, the Department shall follow relevant procedures put in place in order to cater for and assess the details relating to any such data breach promptly and efficiently.
b) The Department shall notify affected individuals of the data breach in accordance with applicable legislation.

7. Approving Authority

The Member of the Executive Council has the responsibility to approve the Access Privacy Policy.

8. Administration of Policy

The administration of this policy shall be vested on the Head of Department who shall ensure employee adhere to this policy.

9. Exceptions/Exemption

Exceptions shall be made on the protection of personal information on the third-party links as the department cannot provide such services.

10. Accountabilities and Responsibilities

10.1. Information Officer

The Information Officer shall be responsible for the following:

a) Taking steps to ensure reasonable compliance with the provision of POPIA.
b) Continually analysing privacy regulations and aligning them with Department personal information processing procedures.
c) Encouraging compliance with conditions required for lawful processing of personal information.

d) Ensuring employees and individual granted access are aware of risks associated with processing of personal information.
e) Addressing all POPIA related requests and complaints made by Department of Social Development's data subjects.
f) Working with the Information Regulator in relation to any ongoing investigations.
g) The Information Officers acts as the contact point for the Information Regulator Authority.

10.2. The Head of Information Management, Systems and Technology

The Head of Information Management, Systems and Technology shall be responsible for the following:

a) Ensuring Information Technology infrastructure, filing systems and devices used for processing personal information meet security standards.
b) Ensuring electronical personal information is kept on designated drives and servers.
c) Ensuring servers containing personal information are stored in a secure location and are backed up and tested.
d) Ensuring personal information being transferred electronically is encrypted.
e) Ensuring servers and computers containing personal information are protected by a firewall.

10.3. Records Management

a) Shall determine retention periods in consultation with the Provincial Archives Unit.
b) Shall provide interventions to ensure record keeping and records management systems comply with National Archives and Records Service Act (Act No. 43 of 1996).
c) Shall ensure records created and received are classified accordingly.

10.4. Security Management

a) Shall be responsible for the physical security of records.
b) Shall be responsible for information security requirements.

10.5. Communications Unit

a) Shall approve and maintain protection of personal information statements and disclaimers.
b) Shall address personal information protection queries from journalists and media.
c) Shall ensure outsourced marketing initiatives comply with POPIA.

10.6. Employees and Individuals Granted Access

a) Shall be required to treat personal information as a confidential business asset.
b) Shall not directly or indirectly disclose personal information they have access to outside of what is provided for in this policy and what is in line with relevant legislation.

c) Shall request assistance from their line manager if unsure about the protection of a data subject's personal information.
d) Shall only process the personal information of a data subject who is a child when such processing is necessary for pursuing legitimate departmental business interests.

10.7. The Head of Department

The Head of Department shall be accountable for the effective implementation and compliance with this policy.

10.8. The Deputy Information Officer

The Deputy Information Officer shall assist the Information Officer in performing his or her duties delegated by the Information Officer including handling PAIA and POPI Act compliance issues.

11. The Member of the Executive Council

The Member of the Executive Council shall be responsible for the approval of this policy.

12. Effective Date of the Policy

This policy shall be implemented from its effective date approval.

13. Monitoring Mechanisms

a) The Department must implement practical steps, such as appointing an information officer, Deputy information and Governance Champion officer to conduct privacy impact assessments.
b) Enforcement requires monitoring access to personal information, implementing security controls, and managing how information is retained or destroyed.
c) Oversight conducted by the Office of the Premier, Information Regulatory supervises compliance and investigates breaches, with individuals able to lodge complaints for inadequate resolution of privacy concerns.
d) Enforcement ensures data subject can request access to, correction of, or deletion of their personal information.

14. Enforcement

14.1. Compliance Assessment and Internal Governance

a) All departmental offices shall undergo an annual assessment to ensure continuous improvement and strict adherence to POPIA compliance requirements.
b) Failure by any employee to comply with the provisions of this Privacy Policy or the POPI Act shall result in internal disciplinary action, conducted in accordance with the departmental Code of Conduct.
c) Statutory Consequences of Non-Compliance.

14.2. The Information Regulator and the South African judicial system may impose the following penalties for serious violations of the POPI Act:

a) Financial Penalties: Administrative fines of up to R10 million.
b) Criminal Prosecution: Responsible parties may face criminal charges, which can result in imprisonment for a period of up to 10 years.
c) Enforcement Notices: The Regulator may issue mandatory notices requiring specific remedial actions, which may lead to significant operational disruptions.
d) Civil Liability: Data subjects reserve the right to institute civil action for damages resulting from the interference with the protection of their personal information.
e) Personal Liability: Individuals in positions of authority (Directors or Information Officers) may be held personally liable for a failure to implement or manage data protection effectively.
f) Reputational Impact: Public disclosure of data breaches can result in a permanent loss of stakeholder trust and damage to the department's institutional reputation.

15. Review of the Policy

The policy shall be reviewed after three years (3) and whenever there are new developments or legislation change.

16. Policy Recommendation and Approval

Recommended/Not Recommended

MR. M. MACHEMBA
HEAD OF DEPARTMENT
EASTERN CAPE DEPARTMENT OF SOCIAL DEVELOPMENT
DATE: 04/05/2026

Approved/Not Approved

MS. B. FANTA
MEMBER OF THE EXECUTIVE COUNCIL
EASTERN CAPE DEPARTMENT OF SOCIAL DEVELOPMENT
DATE: 04/05/2026