Social Development

Gavin Miller

Directorate Research and Information Management

Gavin.Miller@westerncape.gov.za../ Tel.: 021 483 4168

Reference No.: 4/6/2 POPIA Compliance Framework & Privacy Notice

DEPARTMENT OF SOCIAL DEVELOPMENT

POPIA COMPLIANCE FRAMEWORK AND PRIVACY NOTICE

2025- 2026

Revision History

Date	Version	Description	Author
17 February 2025	Draft V1	Annual Review	K Marthinus
29 February 2025	Daft V2	Review	K Marthinus
13 March 2025	Final	Approval	K Marthinus

Table of Content

Definitions

Data subject	Means the identifiable natural/juristic person to whom personal information relates.
Information assets	Means the assets the organisation uses to create, store, transmit, delete and/or destroy information to support its business activities as well as the information systems with which that information is processed. It includes: • All electronic and non-electronic information created or used to support business activities regardless of form or medium, for example, paper documents, electronic files, voice communication, text messages, photographic or video images. • All applications, devices and other systems with which the organisation processes its information, for example telephones, fax machines, printers, computers, networks, voicemail, e-mail, instant messaging, smartphones and other mobile devices ('ICT assets'),
Information custodian	Means the person responsible for defining and implementing security measures and controls for Information and Communication Technology ('ICT') assets.
Information end user	Means a person that interacts with information assets and ICT assets for the purpose of performing an authorised task.
Information officer	Means the Director-General in the case of the Department of the Premier and the Accounting Officer in the case of the other provincial departments.
Information owner	Means a person responsible for, or dependent upon the business process associated with an information asset.
Personal information	Means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to – a) Information relating to the race, gender, marital status, nationality, age, physical or mental health, disability, belief, culture, language and birth of the person. b) Information relating to the education or the medical, financial, criminal or employment history of the person. c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person d) the biometric information of the person. e) the personal opinions, views or preferences of the person. f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence

	g) the views or opinions of another individual about the person; and h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.
Processing	Means any operation or activity or any set of operations concerning personal information, including: a) the collection, receipt, recording, organisation, collation, storage, updating, modification, retrieval, alteration, consultation or use; b) dissemination by means of transmission, distribution or making available in any other form; or merging, linking, as well as restrictions, degradation, erasure or destruction of information.
Special personal information	Means personal information as referred to in section 26 of POPIA, including: a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; b) the criminal behaviour of a data subject to the extent that such information related to- (i) the alleged commission by a data subject of any offence; or (ii) Any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

1. Introduction

The Department of Social Development ("Department") needs to gather and use certain information about individuals and juristic persons (collectively referred to as "data subjects"). These can include clients/customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. This policy describes how this information must be collected, handled and stored to meet the organisation's personal information protection standards and to comply with the law.

This policy must be read with the DSD Information Security Classification System ("ISCS").

2. Purpose

This privacy policy ensures that the Department:

- Complies with the Protection of Personal Information Act, 2013 (Act 4 of 2013) (POPIA).
- Protects the rights of data subjects.
- Is open about how it stores and processes personal information of data subjects, and
- Protects itself from the risks of a security breach.

3. Policy Statement

The organisation is committed to protecting the privacy of data subjects in accordance with the obligations imposed by POPIA. POPIA describes how organisations must collect, handle and store the personal information of data subjects. These rules apply regardless of whether the information is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected fairly, stored safely and not disclosed unlawfully.

POPIA is underpinned by the following important privacy principles that states that personal information must be:

- Processed fairly and lawfully
- Obtained only for specific, lawful purposes
- Adequate, relevant and not excessive
- Accurate and kept up to date
- Held for no longer than necessary
- Processed in accordance with the rights of data subjects
- Protected in appropriate ways, and
- Transferred outside South Africa only to a country or territory that also ensures an adequate level of protection

4. Scope

This policy applies to all the organization's employees and any other person or entity working for or on behalf of the organisation such as:

- interns
- volunteers
- consultants, and
- contractors, suppliers or service providers, including their staff or agents

It governs all business activities that involve the processing of personal information, including special personal information, for or on behalf of this organisation. This can include:

- names of individuals and juristic persons (together with any of the following)
- contact information such as postal and e-mail addresses and telephone numbers
- biographical information such as date of birth, race, gender and marital status
- any identifying number, location information or online identifier
- biometric information such as fingerprints
- educational, medical, financial, criminal or employment history

5. Risks

This policy helps to protect the organisation from some very real security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choices.** For instance, all data subjects should be free to choose how the organisation uses information relating to them where the personal information is not collected, used or shared in terms of a law or an agreement between the data subject and the organisation.
- **Reputational damage.** For instance, the organisation could suffer if hackers successfully gained access to the personal information of data subjects.

6. Responsibilities

Everyone who works for or with the organisation has some responsibility for ensuring that the personal information of data subjects is collected, stored and handled appropriately to ensure the confidentiality, integrity and availability thereof. Each Information End User, Information Owner, business unit and team that handles personal information must ensure that it is handled and processed in line with this policy and the privacy principles.

These people have key areas of responsibility:

a) The **Information Officer** is ultimately responsible for ensuring that the organisation meets its legal obligations.

b) The **Security Manager** is responsible for:

- Keeping the Information Officer updated about information assets and personal information protection responsibilities, risks and issues.
- Reviewing all personal information protection procedures and related policies, in line with an agreed schedule and make recommendations to the Information Officer where applicable.
- Arranging personal information protection training and advice for the people covered by this policy.
- Checking and approving any contracts or agreements with third parties that may collect, handle or store personal information on behalf of the organisation.
- Classifying personal information in line with the WCG Information Security Classification System.
- Maintaining internal procedures to support the effective handling and security of personal information.
- Ensuring that all employees, consultants and others that report to the Department are made aware of and are instructed to comply with this and all other relevant policies.

c) The **Deputy Information Officer(s)** is responsible for dealing with requests from data subjects who want to see the personal information the organisation holds about them (also called 'data subject access requests'). The identity of anyone making a data subject request must be verified before disclosing any personal information.

d) The **Deputy Director Information and Communications Technology (ICT)** in the Directorate Research and Information Management[1] is responsible to monitor for:
- Ensuring all ICT assets used for processing personal information meet capable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the organisation is considering using to process personal information. For instance, cloud computing services.

e) The **Chief Director Business Planning and Strategy** in conjunction with the **Director Business Planning and Monitoring** is responsible for:
- 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.
- Where necessary, working with other business units to ensure all communication initiatives abide by the privacy protection principles.

f) The **Records Manager** is responsible to:
- Monitor the compliance of staff utilizing the approved file plan of the Department to ensure the effective retrieval of records
- Ensure that only staff within and outside records management have access to files

[1] If these functions/some of these functions are provided by a third party (e.g. Ce-I or their service providers) then the management and oversight of the agreement in place between the Department and Ce-I is the responsibility of the [Security Manager/Deputy Information Officer/Other].

- Arrange records in such a manner that minimizes the need to scrutinize the complete file when using a file e.g. by segmenting information on the files
- Ensure that staff adhere to the retention periods of files so that records can be disposed off as per the approved disposal schedule
- Provide training to DSD staff of the safe keeping of electronic records
- Ensure that electronic records are disposed of/ archived in line with the disposal period

g) The **Deputy Director Records and Knowledge Management (Knowledge Manager)** is responsible to:

- Conduct an audit of personal information held by individuals and components
- Compile, update and maintain a Personal Information Register for the Department

7. General Staff Guidelines

a) The only people able to access any personal information covered by this policy should be those who **need it for their work**.

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

d) The organisation **will provide training** to all employees to help them understand their responsibilities when handling personal information.

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

f) In particular, **strong passwords must be used** and they should never be shared.

g) Personal information **should not be disclosed** to unauthorised people, either within the organisation or externally.

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

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

j) Line managers should seek the assistance of the Deputy Information Officers if they are unsure about any aspect of the protection of personal information. The DIO may consult with the Security Manager and or other DIO's in a Departmental POPIA Forum.

k) **Note** that legal services in the Department of the Premier can be approached for clarification.

7.1 Collection

The organisation collects information to support its service delivery mandate. Personal information is collected directly from data subjects where practical and always in compliance with POPIA. The types of information and the purposes for which personal information is collected is set out in

the organisation's Privacy Notice.[2] https://www.westerncape.gov.za/social-development/service/dsd-paiapopia. See **Annexure A** for the amended Privacy Notice for the Departments.

7.2 Classification

The Information Officer classifies information in accordance with its legal requirements, value, criticality and sensitivity to unauthorised disclosure, modification or loss in terms of the DSD Information Security Classification System ("ISCS")]

- Personal information is usually classified as **CONFIDENTIAL**.
- Special personal information and children's information is usually classified as **SECRET**.

7.3 Use

When personal information is accessed and used it can be at the greatest risk of loss, corruption or theft. Therefore:

a) When working with personal information, employees should ensure **the screens of their computers are locked** when left unattended.
b) Personal information should **not be shared informally**.
c) All personal information sent over **e-mail** (as an attachment or in an email text) should be considered sensitive and protected as such. It should not be sent to someone outside of the organisation unless it has been cleared by the line manager. This includes forwarding such e-mails to an employee's own personal e- mail account.
d) Before sending e-mail to a co-employee confirm with the line manager that the recipient is allowed to have access thereto as not all users within the organisation have access to the same information.
e) Data must be **encrypted before being transferred electronically**. The [Security Manger/ IT Manager/Other] can explain how to send data to authorized external contacts.
f) Personal information should **never be transferred outside of South Africa** without confirmation by the Security Manger that the country where it is transferred to ensures an adequate level of protection of personal information.
g) Employees **should not save copies of personal information to their own computers.** Always access and update the central copy of any personal information.

7.4 Storage

These rules describe how and where personal information should be safely stored. Questions about storing personal information safely can be directed to the relevant Deputy Information Officer.

When personal information is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to personal information that is usually stored electronically but has been printed out for some reason:

[2] Create a hyperlink to this Privacy Notice/ include details where it can be obtained.

a) When not required, the paper or files should be kept **in a locked drawer or filing cabinet.** Where the information is classified as **SECRET access** to the environment should be **restricted** and logged.
b) Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer or photocopier.
c) **Printouts that contain personal information should be shredded immediately** and disposed of securely when no longer required.

When personal information is **stored electronically**, it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts:

a) All electronic storage requires access controls and file protection mechanisms such as **encryption**.
b) All electronic access must be **logged**.
c) Personal information should only be stored on **designated drivers and servers** and should only be uploaded to **approved cloud computing services.**
d) Storing personal information on any other physical devices, including but not limited to USB drives (memory sticks), external hard drive, CD or DVD must be **pre-approved** by the relevant Deputy Information Officer.
e) If personal information is **stored on removable media** (like a memory stick, external hard drive, CD or DVD) the files should be encrypted, password protected and the media should be locked away securely when not being used.
f) USB drives (memory sticks) that are found or have been handed out as a promotional item should not be plugged into any computer as these devises may contain hidden malware or viruses.
g) All lost or stolen devices (including removable media) must immediately be reported to the line manager [and the Security Incident Notification document completed].[3] https://inforegulator.org.za/wp-content/uploads/2020/07/FORM-SCN1-Security-Compromises-Notification-Fillable-Formpdf.pdf
h) Servers containing personal information should be **sited in a secure location,** away from general office space.
i) Electronic files that contain personal information should be **backed up frequently.** Those backups should be tested regularly in line with the organization's standard backup procedures.
j) All servers, computers and other electronic devices containing personal information should be protected by **approved security software and a firewall.**

7.5 Data accuracy

The law requires the organisation to take reasonable steps to ensure personal information is kept accurate and up to date. The more important it is that personal information is accurate, the greater the effort the business unit should put into ensuring its accuracy. It is the responsibility of all employees who work with personal information to take reasonable steps to ensure that it is kept as accurate and up to date as possible.

[3] Notification to the Information Regulator of any Security Breaches.

a) Electronic files that contain personal information will be held in **as few places as necessary.** Staff should not create any unnecessary additional data sets.
b) Staff should **take every opportunity to ensure personal information is updated.** For instance, by confirming a client's details when they call.
c) The organisation will make it **easy for data subjects to update their personal information** the organisation holds about them. For instance, via its website.
d) Personal information should be **updated as inaccuracies are discovered.** For instance, if a client can no longer be reached on their stored telephone number, it should be removed from the database.

7.6 Disposal

Working papers and copies that may be disposed of in terms of a general disposal instruction must be disposed of by using a secure disposal container or shredder. Copies of personal information, including special personal information, classified as **SECRET** that is **stored electronically** must either be permanently destroyed or overwritten. The disposal of all original files and electronic files must be performed in accordance with the organisation's **Records Management Policy**.

8. Data Subject Access Requests

All data subjects whose personal information is held by the organisation are entitled to:

- Ask **what information** the organisation holds about them, why and with who it is shared.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the organisation is **meeting its obligations in terms of POPIA.**

If a data subject contacts the organisation requesting this information this is called a data subject access request. Subject access requests from data subjects should be referred to the relevant Deputy Information Officer.

9. Disclosing (sharing) Personal Information

Personal information can be shared internally and with external service providers like for training purposes

9.1 Internal disclosure

In general, personal information is shared within the organisation where legally permitted for reasonable and appropriate business purposes. However, even within the organisation access is restricted to those employees or third parties who need access to carry out their assigned functions.

9.2 External disclosure

External to the organisation disclosure is only made pursuant to an agreement, as permitted or required by law or legal process, or with the consent of the data subject. POPIA allows personal information to be shared if it involves **national security or criminal activities without the consent** of the data subject. Under these circumstances the requested personal information will be disclosed.

However, the Deputy Information Officer in consultation with the Security Manager will ensure that the request is legitimate and in line with POPIA, seeking assistance from Legal Services where necessary.

10. Notification to Data Subjects[4]

The organisation aims to ensure that data subjects are aware that their personal information is being processed, and that they understand how the personal information is being used, what their rights are in terms of POPIA and how to exercise their rights. To these ends, the organisation has a privacy notice, setting out how personal information relating to a data subject is collected and used by the organisation. This is available on request. A version of this notice is also available at *https://www.westerncape.gov.za/social-development/service/dsd-paiapopia*.

11. Enforcement

Non-compliance with this policy by the organisation's employees will be dealt with in accordance with the [Disciplinary Code/Regulations] of the organisation. Consequences may include disciplinary action up and to termination of employment, and/or legal proceedings to recover any loss or damage to the organisation, including the recovery of any fines or administrative penalties imposed by the Information Regulator on the organisation in terms of POPIA.

Non-compliance with the policy by any other third-party processing personal information on behalf of the organisation will be dealt with in accordance with the agreement entered into between the organisation and such third party. Consequences may include the recovery of any fines or administrative penalties imposed by the Information Regulator on the organisation in terms of POPIA.

12. Review and Update

This policy will be reviewed and updated at least annually. If any regulatory or business changes result in a significant addition or change to the nature or handling of personal information that may require a review of this policy the changes will be guided by the Security Manager/Deputy Information Officers and approved by the Information Officer.

Any questions and requests to update the policy should be directed to the Director Research and Information Management.

[4] See Chapter 8 for Notice templates.

13. Recommendation and Approval

In line with the above-mentioned paragraphs, it is recommended that the:

13.1 Amended POPIA Compliance Framework 2025-26 for the Department is approved; and

13.2 Amended POPIA Privacy Notice 2025-26 attached as Annexure A, is approved

Robert Macdonald

Digitally signed by Robert Macdonald
Date: 2025.04.11 13:50:10 +02'00'

HEAD OF DEPARTMENT: SOCIAL DEVELOPMENT

Dr R Macdonald

Social Development

Gavin Miller

Directorate Research and Information Management

Gavin.Miller@westerncape.gov.za../ Tel.: 021 483 4168

Reference No.: 4/6/2 POPIA Compliance Framework & Privacy Notice

DEPARTMENT OF SOCIAL DEVELOPMENT: POPIA PRIVACY NOTICE: 1 APRIL 2025 – 31 MARCH 2026

ANNEXURE A: DSD POPIA PRIVACY NOTICE

The Department of Social Development respects and protects your privacy

What is this notice and who does it apply to?

This is a general notice that explains:

- Who we collect personal information from;
- What personal information we collect;
- Why we collect your personal information;
- How we use your personal information; and
- What rights you have in relation to your personal information.

This notice also explains:

- How you can access the information we hold about you and ask for that information to be corrected; and
- How you can make a complaint about the way we have handled your personal information.

This general notice applies to all persons (both natural and juristic, like companies and close corporations) whose personal information we collect, regardless of form and medium. This includes our employees, consultants, agents, service providers.

It applies to all our services and related websites.

You must read this privacy notice together with the rules for using our website (including our disclaimer), our copyright license and any other notices and policies that may apply to you. (For example, the WCG IT End User Policy).

In addition to this general notice we may need to explain specific privacy practices in more detail. In such circumstances, we develop and provide separate privacy notices to describe how we will handle the personal information that we collect.
For example, where we ask you to provide personal information in relation to your employment or in a public submission to a policy proposal, we will provide you with a privacy notice at the time of collection or as soon as practicable afterwards. These privacy notices explain our personal information handling practices in relation to that particular purpose or activity.

The contact details and addresses of the Departments offices are at the bottom of this notice.

The Protection of Personal Information Act, 2013 (POPIA)

The Protection of Personal Information Act, 2013 (POPIA) protects personal information of natural and juristic persons and requires the Department of Social Development to comply with the eight minimum conditions set out in the Act.

'**Personal information**' is information or an opinion about an identified person, or an individual who is reasonably identifiable.
Personal information includes '**special** personal information', which is a particular category of personal information. While we recognise that protecting all personal information is important in gaining and maintaining your trust, special personal information is often afforded a higher level of protection.

Collection of personal information from citizens, employees, NPO's and suppliers

We collect and hold a broad range of personal information in records relating to:

- Correspondence from members of the public or organisations addressed to us or our Provincial Minister;
- Correspondence from other Provincial Ministers and organs of state;
- Employment and personnel matters relating to staff and contractors;
- Facilitating appointments;
- Facilitating meetings;
- Administering programs for which the Department is responsible;
- Research we have commissioned;
- Contract management (including Transfer Payment Agreements & Business Plans);
- Complaints (including privacy complaints) and feedback provided to us;
- Requests under the Promotion of Access to Information Act, 2000 (PAIA);
- Legal advice provided by internal state law advisors and external lawyers; and
- The performance of legislative and administrative functions.

We collect personal information in a variety of ways. These include:

- Correspondence and submissions;
- Paper-based forms;
- Online (web-based forms and e-mail); and
- Phone calls, faxes and face to face meetings.

We often collect personal information directly from you. However, in some circumstances we may also collect information about you from another organ of state or organisation.

- Certain third-party service providers may collect or check information from or about you on our behalf. For example, where we use external employment agencies, vetting agencies, credit bureaus, lawyers, accountants, consultants, professional bodies, banks, travel agencies, non-government organisations and security companies.
- We work with public bodies or organs of state such as local, provincial and national government departments, municipalities, public universities and state-owned companies, which may collect or check information from or about you on our behalf.
- We only collect personal information where that information is reasonably necessary for, or directly related to, one or more of our functions or activities.

We collect personal information from and about:

- **Visitors to our website**:
  - We collect information that you give to us directly via our website contact forms.
  - We also use common technologies (including 'cookies') to anonymously and automatically track website use and improve user experience. You can usually disable these if you prefer. Our website privacy notice has more information.
- **Our job applicants, bursary applicants, intern applicants and employees**:
  - We collect information from you when you apply for a job, internship or bursary and if you are successful and we employ you, give you an internship or a bursary.
  - We may also collect information about you from third parties, like educational bodies or previous employers.
  - We also collect information about employees' and interns' use of email and the internet to monitor and review e-mail and internet activity, where we believe it is reasonable and necessary to detect abuse or unlawful activity on the department's resources. You cannot expect privacy in this regard.
- **Our suppliers, service providers, contractors, consultants and NPO's**:
  - We collect information from you when you apply to be listed on our supplier database and bid to supply goods or services to us.
  - We may also collect or check information about you from various private or public bodies, such as banks or tax authorities.
- **Our citizens and users of the Departments public services and facilities**:
  - We collect information you give us when you send us a letter, an email or text message, or when you use social media or our call centre to contact us.
  - We also collect personal information when it is directly relevant to the specific public services we provide to you.
  - We also collect information from visitors to our buildings and facilities in terms of the Control of Access to Public Premises and Vehicles Act, 1985.

Types of personal information we collect and use

The personal information we collect and hold varies depending on what we need to perform our functions and responsibilities. It may include:

- Your name, address and contact details (for example your phone number or email address);
- Information about your identity (such as date of birth, country of birth, passport details, visa details and driver's licence);
- Information about your personal circumstances (for example age, gender, marital status and occupation);
- Information about your financial affairs (for example payment details, bank account details, and business and financial interests);
- Information about your employment (for example applications for employment, work history, referee comments and remuneration); and
- Government identifiers.

We do not necessarily collect all of this information from every person but only where it is necessary.

Special personal information

We may also collect 'special personal information' which is a subset of personal information under the POPIA.

Special personal information includes information about the following:

- Your health;
- Your membership of a professional or trade association, or a trade union;
- Your racial or ethnic origin;
- Your disability status;
- Criminal activities you may have been involved in; and
- Your biometrics (including photographs and voice or video recordings of you).

Generally, we will only collect special personal information if its collection is reasonably necessary for, or directly related to, one or more of our functions or activities or the collection is required or authorised by law. For example, we collect special personal information such as race and disability to inform the development of a workforce plan. We require employees to complete the EEA 1 form prescribed by the Employment Equity Act, 1998. We ensure that the contents remain confidential and only use the information to comply with previously mentioned act.

We collect general personal and contact information about our employees, suppliers, clients, NPO's and users of our public services and facilities.

- **Job applicants and employees:** We usually collect detailed personal information about your educational, employment, financial and criminal background, and any other relevant information such as images of you, fingerprints, drivers license details, vehicle registration number, tax number and bank account details. If we employ you, we will also allocate you a unique identifier called a PERSAL number. We may also need further information about matters such as health issues and family members, where relevant to the employment relationship.
- **Suppliers, service providers, contractors and consultants**: We often collect detailed personal information about your qualifications, experience or suitability as a supplier, and other relevant information such as bank account details and VAT number. We may also need further information relevant to the business relationship, such financial statements or information about solvency.
- **Visitors to our buildings and facilities**: We usually collect close circuit television (CCTV) images (and audio recordings, where applicable) of visitors to The Department buildings and facilities, as well as names, identity numbers and contact details.
- **NPO's**: We collect the names and details of citizens that make use of the NPO services funded by the Department for monitoring, evaluation and to improve our services to those most in need of care and protection.

Why components of the Department collect specific information

Office of the Minister

- Provides political and legislative interface between government, civil society and all other relevant stakeholders.
- Respond to Parliamentary Questions and answers

Corporate Management Services

- Capacity building of social work and related professions.
- Manage DSD infrastructure matters
- Coordinate the provision of human resource matters such as recruitment and training between DSD and the Department of the Premier
- Deals with PAIA / POPIA requests

Financial Management

- Timeous payment of invoices within 30 days for service providers
- Provision of accounting services
- Render an internal control function
- To monitor and evaluate Supply Chain Management (SCM) and asset management compliance

Business Planning and Monitoring

- Render a strategic communication service to components/ regions and facilities

Research and Information Management

- Conduct and report on research
- Conduct population management surveys and research
- Provide record management services
- Implementation of knowledge management
- Provide a library service to staff
- Deals with PAIA / POPIA requests

Social Welfare and Restorative Programmes

- Provide service directly or through the NPO sector to citizens such child protection. Disabilities and Gender Based Violence
- Provide own services such as care facilities for children and youth and substance abuse
- Capacitate organisations to build resilient communities

Children and Families and Vulnerable Groups

- Provide services directly or through the NPO sector to citizens such as child protection and services to families
- Provide services directly or through the NPO sector to vulnerable groups such as disabled and older persons
- Capacitate organisations to build resilient communities

Community and Partnership Development

- Provide community development service through the NPO sector to citizens such as feeding supports programmes, services to youth, and social relief of distress
- Create and sustain strategic partnerships and manage institution capacity building

Service Delivery Management and Coordination in regional offices

- Provide social welfare and community development services directly to citizens through six (6) regional offices and fourty-five (45) service delivery areas
- Provide an after-hour child protection hotline service

Use and disclosure of personal information

We routinely use your personal information:

- To communicate and manage our relationship with you;

- To provide you with public services, as required or allowed by law;
- To manage security and access control to our buildings and facilities; and
- For record keeping and other administrative purposes, as required by law.

We will not provide your personal information to anyone else unless you consent thereto or one of the following exceptions applies:

- You would reasonably expect us to use the information for that purpose;
- It is legally required or authorised, such as by a law, or a court or tribunal order;
- It is reasonably necessary for an enforcement-related activity;
- We reasonably believe that it is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety;
- We have reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to our functions or activities has been, is being or may be engaged in and we reasonably believe that it is necessary for us to take appropriate action in relation to the matter;
- It is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim; or
- The information is used only for historical, statistical or research purposes and is not published in an identifiable form.

- When we share your personal information with selected service providers who work on our behalf, for specific defined purposes related to public services we provide we will ensure that appropriate protections of your personal information are in place with these third parties, in accordance with our obligations under the POPIA.
- We are very careful with special personal information, and where practical, we usually group personal information together as aggregated data so that individuals cannot easily be identified.

Unless we have your clear informed consent or the law clearly allows us in certain limited circumstances, we will not:

- Sell or rent personal information;
- Use your personal information for purposes that are different, unusual or unexpected in relation to the reason for collecting it in the first place; or
- Share your personal information with third parties in circumstances other than the ones we have referred to above.
-

Storage and data security

We respect and protect your privacy and store your personal information according to generally accepted information security practices. We take all reasonable steps to protect the personal information held in our possession against loss, unauthorised access, use, modification, disclosure or misuse. The Department will act promptly with any accidental or unauthorised disclosure of personal information.

Storage of personal information (and the disposal of information when no longer required) is managed in accordance with the Western Cape Government records management regime as provided for in the Provincial Archives and Records Service Act of the Western Cape, 2005. When the personal information we collect is no longer required, we delete or destroy it in a secure manner, unless we are required to maintain it because of a law, or court or tribunal order.

Where a breach of personal information occurs, we will notify the Information Regulator and affected individuals as required. We will aim to provide you with timely advice to ensure you are able to manage any loss—financial or otherwise—that could result from the breach

Your choices and consent in connection with your personal information

- We try to obtain your consent to collect and use your personal information, where practical.
- You do not normally have to give us personal information, but if you do not, we may not be able to communicate with or provide government services to you. You may also ask us not to send you unsolicited messages (opt-out), but then we cannot tell you about public services that may be important to you.
- You may access personal information we hold about you and ask us to correct or delete any that is wrong, irrelevant, out of date, misleading and so on. But we may check your identity before giving you access. For more information, please read our manual as required by the Promotion of Access to Information Act 2000 (our PAIA/ POPIA manual available here. *https://www.westerncape.gov.za/social-development/service/dsd-paiapopia.*

You also have certain rights to withdraw consent or object to us using your personal information under POPIA, but these rights are limited. For example, if the purpose for which your personal information was requested initially does not exist anymore you may request that the information may no longer be used. We can decline your request to delete the information from our records if other legislation requires us to retain the information.

Privacy Complaints

- If you feel we are not dealing with your personal information fairly and lawfully, you may complain to the Information Regulator at **JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001. P.O Box 31533, Braamfontein, Johannesburg, 2017,** Tel: +27(0) 10 023 52441/42 Email: POPIAComplaints@inforegulator.org.za or enquiries@inforegulator.org.za
- Please first give us a chance to resolve any complaint by contacting us at the contact details provided below.
- Your complaint should include a brief description of what happened, when it happened and what personal information was affected.

How to contact us to complain or ask questions about the Privacy Notice or your personal information

Email:	HOD.DSD@westerncape.gov.za
Tel:	021 483 3083
Responsibility:	Head of Department
Post:	Information Officer, Department of Social Development, 14 Queen Victoria Street, Cape Town, Private Bag x9112, Cape Town, 8001
Visit us in person:	14 Queen Victoria Street, Union House, Cape Town, 8001

Email:	Gavin.Miller@westerncape.gov.za
Tel:	021 483 4168
Responsibility:	Head Office
Post:	Deputy Information Officer, Department of Social Development, 48 Queen Victoria Street, Cape Town, Private Bag x9112, Cape Town, 8001
Visit us in person:	14 Queen Victoria Street, Union House, Cape Town, 8001

Email:	Annemie.vanReenen@westerncape.gov.za
Tel:	021 483 9392
Responsibility:	Regional Offices x 6
Post:	Deputy Information Officer, Department of Social Development, 48 Queen Victoria Street, Cape Town, Private Bag x9112, Cape Town, 8001
Visit us in person:	14 Queen Victoria Street, Union House, Cape Town, 8001
Email:	Petronell.VanWyk@westerncape.gov.za
Tel:	021 483 6741
Responsibility:	Head Office
Post:	Deputy Information Officer, Department of Social Development, 48 Queen Victoria Street, Cape Town, Private Bag x9112, Cape Town, 8001
Visit us in person:	14 Queen Victoria Street, Union House, Cape Town, 8001
Email:	Marshionette.Jonkerman@westerncape.gov.za
Tel:	2721-8266040
Responsibility:	Directorate Facility Management
Post:	Deputy Information Officer, Department of Social Development, R101, De Novo Treatment Centre, Kraaifontein, 7570
Visit us in person:	R101, Old Paarl Road, De Novo HUB, Kraaifontein, 7570

DSD Customer Care Helpline

Telephone: 021 483 5045 or 0800-250-220

Email: SD.CustomerCare@westerncape.gov.za

You can also request paper copies of this privacy notice or any of the documents referred to in this document at any of the offices listed above

WCG Contact Centre

Telephone: 0860 142 142

Email: services@westerncape.gov.za