Department of Social Development
Gavin Miller
Directorate Research and Information Management
Gavin.MIller@westerncape.gov.za | Tel: 021 483 4168

POPIA FRAMEWORK AND POLICY

Reference No.: 4/6/2 POPIA Privacy Notice

DEPARTMENT OF SOCIAL DEVELOPMENT

POPIA COMPLIANCE FRAMEWORK AND POLICY

Version 02/2022

Date of publication: 08/04/2022

Revision History

Date	Version	Description	Author
7 July 2021	01/2021	Drafting of Privacy Notice	G Miller
8 April 2022	02/2022	Annual review	G Miller

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 c) 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.

Western Cape Government

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 WCG Information Security Classification System ("ISCS"). Definitions appear at the end for the meaning of terms used in this policy.

2. Purpose

This privacy policy ensures that the organisation:

- 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 organisation'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 Information Officer, Knowledge 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.

[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].

- 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
- 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

g) The **Knowledge Manager** is responsible to:

- Conduct an audit of personal information held by individuals and components
- Provide training to DSD staff of the safe keeping of electronic records
- Liaise with the Records Manager to ensure electronic records are disposed of/ archived in line with the disposal period

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]

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 WCG Information Security Classification System ("ISCS")]

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

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

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:

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]
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 organisation'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

[3] Create a hyperlink to where this document can be accessed.

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.

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/assets/departments/social-development/popia_dsd_privacy_notice.pdf

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

[4] See Chapter 8 for Notice templates.

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.

13. Recommendation and Approval

In line with the above-mentioned paragraphs the Private Policy Notice for the Department of Social Development is herewith approved

HEAD OF DEPARTMENT: SOCIAL DEVELOPMENT

DR ROBERT MACDONALD

Date: