Western Cape Government
Cultural Affairs and Sport

**File No: 8/5/8/P**

# Departmental Privacy Policy

**Document Version Control**

| DATE | AUTHOR | VERSION NUMBER | REVISION DETAILS |
|---|---|---|---|
| November 2020 | Head: Records Management | **1.0** | |

**Recommendation**

| DESIGNATION | NAME | SIGNATURE | DATE |
|---|---|---|---|
| Director: Strategic and Operational Management Support | **Shaun Julie** |  | 19.02.2021 |

**Approval**

| DESIGNATION | NAME | SIGNATURE | DATE |
|---|---|---|---|
| Head of Department: Cultural Affairs and Sport | **Brent Walters** |  | 26/02/2021 |

## Contents

## 1. INTRODUCTION

The Department of Cultural Affairs and Sport (DCAS) needs to gather and use 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 department has a relationship with or may need to contact. This policy describes how this information must be collected, handled and stored to meet the department's personal information protection standards and to comply with the requirements of the **Protection of Personal Information Act, 2013 (Act 4 of 2013)**.

**This policy must be read with the:**

- Western Cape Government Information Security Framework, 2014
- Western Cape Government IT End User Policy, 2015
- Departmental Security Policy, 2017
- The Provincial Archives and Records Service of the Western Cape Act, 2005 (Act 3 of 2005)
- Regulations relating to the Provincial Archives and Records Service of the Western Cape, Regulation (P.N.122/2006)
- Minimum Information Security Standards (MISS), 1996
- Departmental Records Management Policy, 2018
- Western Cape Government Social Media Policy, 2014 as well as a Departmental Guideline on use of Social Media, 2016.

## 2. DEFINITIONS

| | |
|---|---|
| **Data subject** | Means the identifiable natural/juristic person to whom personal information relates. |
| **Information assets** | Means the assets the department 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.<br><br>It includes:<br>• 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.<br>• All applications, devices and other systems with which the department 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** | The Head of the Department. |
| **Information owner** | Means a person responsible for, or dependent upon the business process associated with an information asset. |
| **Security Manager** | The Security Manager for the Department of Cultural Affairs and Sport |
| **Personal information** | Means information relating to an identifiable, living, natural person, and were it is applicable, an identifiable, existing juristic person, including, but not limited to –<br>a) Information relating to the race, gender, marital status, nationality, age, physical or mental health, disability, belief, culture, language and birth of the person;<br>b) Information relating to the education or the medical, financial, criminal or employment history of the person;<br>c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;<br>d) the biometric information of the person;<br>e) the personal opinions, views or preferences of the person;<br>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;<br>g) the views or opinions of another individual about the person; and<br>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:<br>a) the collection, receipt, recording, department, collation, storage, updating, modification, retrieval, alteration, consultation or use;<br>b) dissemination by means of transmission, distribution or making available in any other form; or<br>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 the Protection of Personal Information Act, 2013 ("POPIA"). |

## 3. PURPOSE

This policy ensures that the Department of Cultural Affairs and Sport:

- Complies with the requirements of 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.
- Protects itself from the risks of a security breach.

## 4. POLICY STATEMENT

4.1 The Department of Cultural Affairs and Sport is committed to protecting the privacy of data subjects in accordance with the obligations imposed by the POPIA. The POPIA describes how the department 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 requirements of the POPIA Act, personal information must be collected fairly, stored safely and not disclosed unlawfully.

4.2 The POPIA is underpinned by the following important privacy principles; i.e. personal information must:

- Be processed fairly and lawfully.
- Be obtained only for specific, lawful purposes.
- Be adequate, relevant and not excessive.
- Be accurate and kept up to date.
- Not be held for longer than necessary.
- Processed in accordance with the rights of data subjects.
- Be protected in appropriate ways.
- Not be transferred outside South Africa unless that country or territory also ensures an adequate level of protection.

## 5. SCOPE

5.1 This policy applies to all Department of Cultural Affairs and Sport employees and any other person or entity working for or on behalf of the department such as:

- Interns.
- Volunteers.
- Consultants.
- Contractors, suppliers or service providers, including their staff or agents.

5.2 It governs all business activities that involve the processing of personal information including special personal information, for or on behalf of the department. This can include but is not limited to:

- 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.

## 6. RISKS

This policy helps to protect the Department of Cultural Affairs and Sport from 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 department uses information relating to them where the personal information is not collected, used or shared in terms of a law, an agreement between the data subject and the department or to protect a legitimate interest of the department or that of a third party or the data subject.
- **Reputational damage.** For instance, the department could suffer if hackers gained access to the personal information of data subjects.

## 7. RESPONSIBILITIES

Everyone who works for or with the Department of Cultural Affairs and Sport 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 Department of Cultural Affairs and Sport meets its POPIA 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.
- 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 department.
- Dealing with requests from data subjects who want to see the personal information the department 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.

**c) The Securty Manager in liaison with CEI is responsible for:**

- Ensuring all Information and Communications Technology (ICT) assets used for processing personal information meet security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the department is considering using to process personal information.

**d) The Records Manager is responsible for:**

- Maintaining internal procedures to support the effective handling and security of personal information.
- Reviewing all personal information protection procedures and related policies, in line with an agreed schedule and make recommendations to the Security Manger where applicable.
- Ensuring that all employees, consultants and others that report to the Information owner are made aware of and are instructed to comply with this and all other relevant policies.

**e) The Director for Strategic and Operational Management Support (SOMS) 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.

## 8. 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**.

Personal information **should not be shared informally** and must never be shared over social media accounts such as Facebook, LinkedIn, Google Plus, etc. The Social Media Policy is available on request.

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

c) The Department of Cultural Affairs and Sport **will provide annual training** to all employees to help them understand their responsibilities when handling personal information.

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

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

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

g) 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.

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

i) Line managers should seek the assistance from the Security Manager or consult Legal Services within the Department of the Premier if they are unsure about any aspect of the protection of personal information.

### 8.1 Collection

The Department of Cultural Affairs and Sport collects information to support its service delivery mandate. Personal information is collected directly from data subjects where practical and always in compliance with the requirements of the POPIA.

### 8.2 Classification

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

- Personal information is usually classified as **CONFIDENTIAL**.
- Special personal information, a subset of personal information that may lead to harassment or victimisation such as race, political or religious beliefs and children's information is usually classified as **SECRET**.

### 8.3 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 department unless it has been cleared by the line manager and Security Manager. This includes forwarding such e-mails to an employee's own personal e-mail account.

d) Before sending an 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 department have access to the same information.

e) Data must be **encrypted before being transferred electronically**. The Security Manager or IT Support Manager can explain how to send data to authorised external contacts.

f) Personal information should **never be transferred outside of South Africa** without confirmation by the Information Officer that the country where it is transferred to ensures an adequate level of protection of personal information.

### 8.4 Storage

These rules describe how and where personal information should be safely stored. Questions about storing personal information safely can be directed to the Security Manager.

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 steel 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, photocopier or unattended desk.

c) **Printouts that contain personal information should be shredded immediately** and disposed of securely when no longer required.

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

e) All electronic storage requires access controls equal to those in production and file protection mechanisms such as **encryption** should be employed.

f) All electronic access must be **logged**.

f) Personal information should **NOT** be stored on designated drives and servers, and should only be uploaded to the MyContent Enterprise Content Management (ECM) system.

g) Storing personal information on any other physical devices, including but not limited to USB drives (memory sticks), external hard drive, CD or DVD is not allowed.

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.**

k) All lost or stolen devices (including removable media) must immediately be reported to the line manager [and the Security Incident Notification document completed.

**8.5 Data accuracy**

The POPIA Act requires the Department 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.

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 responsible staff will make it **easy for data subjects to update their personal information that** the department holds about them. For instance, via its website.

d) Personal information should be **updated as inaccuracies are discovered.** For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

### 8.6 Disposal

The disposal of all original files, documents and electronic files must be performed in accordance with the Department of Cultural Affairs and Sport's Records Management Policy.

## 9. DATA SUBJECT ACCESS REQUESTS

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

- Ask **what information** the Department of Cultural Affairs and Sport 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 Department of Cultural Affairs and Sport is **meeting its obligations in terms of the POPIA.**

If a data subject contacts the department requesting this information this is called a data subject access request.

Subject access requests from data subjects should be referred to the Records Manager / Deputy Information Officer.

## 10. DISCLOSING (SHARING) PERSONAL INFORMATION

### 10.1 Internal disclosure

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

### 10.2 External disclosure

External to the Department of Cultural Affairs and Sport, 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.

The 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 Security Manager will ensure that the request is legitimate and in line with the POPIA, seeking assistance from Legal Services, Department of the Premier where necessary.

## 11. NOTIFICATION TO DATA SUBJECTS

The Department of Cultural Affairs and Sport 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 the POPIA and how to exercise their rights.

To these ends, the Department of Cultural Affairs and Sport has a privacy notice, setting out how personal information relating to a data subject is collected and used by the department.

This is available on request.

## 12. ENFORCEMENT

Non-compliance with this policy by the Department of Cultural Affairs and Sport employees will be dealt with in accordance with the Disciplinary Code of the department. Consequences may include disciplinary action, and/or legal proceedings to recover any loss or damage to the department, including the recovery of any fines or administrative penalties imposed by the Information Regulator on the department in terms of the POPIA.

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

## 13. REVIEW AND UPDATE

This policy will be reviewed if any regulatory or business changes result in a significant addition or changes. Any questions and requests to update the policy should be directed to the Security Manager.