



Western Cape
Government

WESTERN CAPE DEPARTMENT OF AGRICULTURE

PRIVACY POLICY

The Protection of Personal Information Act (POPIA) Act 4 of 2013

April 2022

CONTENTS		
NO	CONTENTS	PAGE NO
1	Recommendation and Approval	3
2	Introduction to the Policy	4
3	Purpose of the Policy	4
4	Policy Statement	4-5
5	Scope and applicability	5
6	Definitions	5-7
7	Risks	7
8	Roles and Responsibility	7-8
9	Policy Governance	8
9.1	Departmental Responsibility	8
9.2	Employees' Responsibility	8
9.3	Collection	9
9.4	Classification	9
9.5	Use	9
9.6	Storage	9-10
9.7	Data accuracy	10
9.8	Disposal	11
10	Data Subject access request	11
11	Confidentiality of sensitive data	11
12	Disclosing (Sharing) personal information	11
12.1	Internal Disclosure	11
12.2	External Disclosure	11-12
13	Notification	12
14	Enforcement	12
15	Review	12

TITLE OF THE DOCUMENT: DEPARTMENT OF AGRICULTURE PRIVACY POLICY

REFERENCE NO.: 8/5/8/P Privacy Policy

Document enquiries can be directed to:

Department of Agriculture, Western Cape Government, Muldersvlei Road, Stellenbosch.

Attention: Dr MP Sebopetsa

Designation: Head of Department

Telephone: +27 (021) 808 5006

Email: Mogale.Sebopetsa@westerncape.gov.za

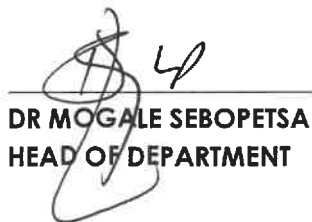
1. Recommendation and approval

The signatories hereof, being duly authorised thereto, by their signatures hereto authorise the execution of the work detailed herein, or confirm their acceptance of the contents hereof and authorise the implementation/adoption thereof, as the case should be, for and on behalf of the parties represented by them.



MS RASHIDAH WENTZEL
CHIEF DIRECTOR: OPERATIONAL SUPPORT SERVICES

29/06/2022
DATE



DR MOGALE SEBOPETSA
HEAD OF DEPARTMENT

29 June 2022
DATE

Revision History

Version	Date	Description	Revision Due
1	April 2022	Privacy Policy	

2. Introduction to the Policy

The Western Cape Department of Agriculture (WCDoA) 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 should need to contact.

This Protection of Personal Information Act 4 of 2013 (POPIA) promotes the protection of personal information processed by public and private bodies, which stipulates that *"the responsible party should ensure that the conditions for lawful processing of personal information and all other measures that give effect to such condition are complied with at all times"*.

The Provincial Top Management (PTM) endorsed the WCG Information Security Classification System (ISCS) in January 2019. The ISCS provides the framework for information security classification. It also provides a standard process to allow Departments to evaluate their information and to determine the appropriate level of security classification that should be applied.

The Department of Agriculture is committed to protect the privacy of its employees, clients and customers. The purpose of the policy is to provide overarching guidelines to protect personal identifiable information, personal financial information and personal health information belonging to WCDoA employees and clients collectively termed ("Protected Information"). This policy describes how information should be collected, handled and stored to meet the department's personal information protecting standards, and to comply with the law.

The policy should be read with the WCG Information Security Classification System (ISCS), WCDoA Security Policy, WCDoA Access Control Directive (Version 4 as of 18 April 2019), WCG IT End User Policy (Version 1.5 as of 09 October 2015) and IT User Account Management Policy (Version 2.1 of 12 May 2016).

3. Purpose

This privacy policy ensures that the department:

- Complies with the 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.

4. Policy statement

The department is committed to protecting the privacy of data subjects in accordance with the obligations imposed by POPIA. POPIA describes how organisations should 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 should be collected fairly, stored safely and not disclosed unlawfully.

POPIA is underpinned by the following important privacy principles. These state that personal information should:

- 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; and
- not be transferred outside South Africa, unless that country or territory also ensures an adequate level of protection.

5. Scope and applicability

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

- Long and short-term interns;
- Volunteers;
- Consultants;
- Contractors, suppliers or service providers, including their staff or agents.

The responsibility for ensuring that protected information is collected, stored and transmitted securely in accordance with the POPIA, is the responsibility of individuals that handle Protected Information, and individuals are responsible for complying with the policy. With respect to the personal information that has been transferred to a contractor or consultant, contractual requirements and reliance upon affirmative statements, as well as independent information security assessment results, are used to provide comparable level of protection.

Furthermore, the policy 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:

- 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; and
- educational, medical, financial, criminal or employment history.

6. 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: <ul style="list-style-type: none"> • All electronic and non-electronic information created or used to support business activities regardless of form or medium, for

	<p>example, paper documents, electronic files, voice communication, text messages, photographic or video images:</p> <ul style="list-style-type: none"> • 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 Head of the Western Cape Department of Agriculture.
Deputy Information Officer	The Deputy Information Officer of a public body or private body is an employee of that public body or private body to whom the Information Officer has delegated their powers and duties in terms of POPIA, read with the provisions of PAIA.
Information Owner	Means a person responsible for, or dependent upon the business process associated with an information asset.
Personal Information	<p>Means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to –</p> <ol style="list-style-type: none"> Information relating to the race, gender, marital status, nationality, age, physical or mental health, disability, belief, culture, language and birth of the person; Information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; the biometric information of the person; the personal opinions, views or preferences of the person; correspondence sent by the person that is implicitly or explicitly of private or confidential nature or further correspondence that would reveal the contents of the original correspondence; the views or opinions of another individual about the person; and 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	<p>Means any operation or activity or any set of operations concerning personal information, including:</p> <ol style="list-style-type: none"> the collection, receipt, recording, organisation, collation, storage, updating, modification, retrieval, alteration, consultation or use; 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.

Protected Information	Means personal identifiable information, personal financial information and personal health information.
Special Personal Information	Means personal information as referred to in section 26 of POPIA.

7. Risks

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

- **Breaches of confidentiality.** For instance, information 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.

8. Roles and Responsibilities

Everyone who works for or with the department 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 should ensure that it is handled and processed in line with this policy and the privacy principles.

Summary of key areas of responsibility:

- a) The **Information Officer** is ultimately responsible for ensuring that the department 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;
 - Arranging personal information protection training and advice for the people covered by this policy; and
 - Checking and approving any contracts or agreements with third parties that should collect, handle or store personal information on behalf of the organisation.
- c) The **Deputy Information Officer** appointed by the **Information Officer** is responsible for 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 should be verified before disclosing any personal information.
- d) The **Information Custodian and delegate/s** are responsible 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; and

- Evaluating any third-party services the organisation is considering using to process personal information. For instance, cloud computing services.
- e) The **Information Owner and delegate/s** are responsible for:
- 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;
 - Reviewing all personal information protection procedures and related policies, in line with an agreed schedule, and make recommendations to the Security Manager/delegate where applicable; and
 - Ensuring that all employees, consultants and others that report to the Information Owner/delegate are made aware of and are instructed to comply with this and all other relevant policies.
- f) The **Departmental Communications Unit** 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; and
 - Where necessary, working with other business units to ensure all communication initiatives abide by the privacy protection principles.

9. Policy Governance

9.1 Departmental Responsibility

The policy is the joint responsibility of all the programmes and sub-programmes within the department.

9.2 Employees' Responsibilities

If any individual learns of the accidental or intentional exposure of Protected Information of employees or clients, he/she is responsible to report the event immediately to his/her line supervisor who should in turn report this to the Security Manager.

- 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 should never be shared over social media accounts such as Facebook, LinkedIn, Google Plus, etc.;
- c) When access to 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 should 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 should 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 Security Manager if they are unsure about any aspect of the protection of personal information.

9.3 Collection

The department 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 department's Privacy Notice.

9.4 Classification

The Information Owner or delegate 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**.

9.5 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 that **the screens of their computers are locked** when left unattended;
- b) Personal information should **not be shared informally**;
- c) All personal information sent via **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 and Security Manager/IT manager/delegate. 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 organisation have access to the same information;
- e) Data should be **encrypted before being transferred electronically**. The Security 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 Security Manager that the country where it is transferred to ensures an adequate level of protection of personal information; and
- g) Employees **should not save copies of personal information to their own computers**. Always access and update the central copy of any personal information.

9.6 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 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 should be protected from unauthorised access, accidental deletion and malicious hacking attempts.

- a) All electronic storage requires access controls equal to those in production, and file protection mechanisms such as **encryption** should be employed;
- b) All electronic access should be **logged**;
- c) Personal information should only be stored on **designated drives 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 drives, CDs or DVDs, should be **pre-approved** by the Security Manager;
- 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 devices may contain hidden viruses;
- g) All lost or stolen devices (including removable media) should immediately be reported to the line manager and the Security Incident Notification document should be completed;
- 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**.

9.7 Data accuracy

The law 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 department will make it **easy for data subjects to update their personal information** 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.

9.8 Disposal

Working papers, and copies that should be disposed of in terms of a general disposal instruction, should 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**, should either be permanently destroyed or overwritten.

The disposal of all original files and electronic files should be performed in accordance with the department's Records Management Policy.

10. 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 whom it is shared;
- Ask **how to gain access** to it;
- Be informed on **how to keep it up to date**; and
- Be informed on how the organisation is **meeting its obligations in terms of POPIA**.

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

11. Confidentiality of Sensitive Data

Protected Information regardless of its origin, form or format, transmission method or storage location or format, is to be kept secure and confidential. Only authorised individuals that have an established business need are allowed to access, receive, view or discuss Protected Information.

Any WCDoA employees found to violate confidentiality in relation to this Policy, will be subjected to discipline up to, and including immediate termination.

All WCDoA employees are required to obtain written consent from all affected parties prior to disclosure of sensitive information to a third-party entity regardless of the format of the disclosure (verbally, in writing or electronically), unless authorised by law.

12. Disclosing (sharing) personal information

12.1 Internal disclosure

In general, personal information is shared within the department 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.

12.2 External disclosure

External to the department, 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 Security Manager or Deputy Information Officer will ensure that the request is legitimate and in line with the POPIA, seeking assistance from Legal Services, Department of the Premier/other where necessary.

13. Notification to data subjects

The department 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 this end, the department 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 on the following webpage, [WCDoA webpage](#).

Links: (Link to be added when website is fully functional).

14. Enforcement

Non-compliance with this policy by the department's employees will be dealt with in accordance with the Disciplinary Code/Regulations of the department. Consequences should include disciplinary action up to and to termination of employment, 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 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 and such third party. Consequences should include the recovery of any fines or administrative penalties imposed by the Information Regulator on the organisation in terms of POPIA.

15. Review and Update

This policy will be reviewed and updated annually.

If any regulatory or business changes result in a significant addition or change to the nature or handling of personal information that should require a review of this policy, the changes will be developed by the Security Manager/delegate and approved by the Information Officer.

Any questions and requests to update the policy should be directed to the Security Manager.