Peel Development Commission

ORG - 10 Privacy Policy

Policy Reference	ORG-10
Associated Policies	ORG-01 Code of Conduct for Board Members ORG-02 Code of Conduct for Employees ORG-04 Public Interest Disclosure ORG-05 Records Management ORG-08 Complaints CIT-02 Freedom of Information CIT-08 IT Acceptable Use & Security
Associated Documents	DPIRD Privacy Policy Information Privacy Principles (IPPs) Guidelines Collection Notice Procedure Privacy Impact Assessment Procedure Privacy Complaints procedure Privacy Statement
Associated Legislation	Privacy and Responsible Information Sharing Act 2024 Criminal Code Act 1913 Privacy Act 1988 (Federal) Freedom of Information Act 1992 Freedom of Information Regulations 1993 Information Commissioner Act 2024 State Records Act 2000 Regional Development Commissions Act 1993 Public Sector Management Act 1994
Policy Owner	Director Regional Development
File Reference	GR09-010
Issued Date	1 June 2007
Last Review Dates	18 May 2021, 25 June 2019, 23 August 2023, 19 August 2025; 6 July 2026
Next Review Date	6 July 2028

Introduction

Western Australia introduced the *Privacy and Responsible Information Sharing Act 2024* (PRIS Act) on 1 July 2026, which aims to better protect personal information and improve the responsible sharing of government data and will:

- Set clear principles and standards for how government agencies collect, use, store, and share your personal information.
- Allow agencies to share information only if they follow clear principles for risk, decision-making, and transparency.
- Ensure Aboriginal people are involved when sharing data that affects Aboriginal people and communities.

The PRIS Act applies to employees and all persons conducting business or activities on behalf of WA public sector entities, including the Peel Development Commission (Commission), including service providers, contractors and volunteers.

The Chief Data Officer, within the Department of the Premier and Cabinet, will oversee government information sharing under the PRIS Act and from 1 January 2027, where all public sector agencies must start reporting all serious data breaches.

This policy is based on the PRIS Act and the Federal *Privacy Act 1988,* which sets out 13 Privacy Principles. The type of privacy covered by the Privacy Act is the protection of peoples' personal information.

Public sector employees may have access to official, sensitive, confidential and commercially significant information not available to the public. It is essential that as Commission staff we respect the confidentiality of information and not use it for personal benefit or gain and that government policy is adhered to.

Section 9 of the *Public Sector Management Act 1994* requires all public sector bodies and employees to act with integrity in the performance of official duties and to be scrupulous in the use of official information.

Section 81 of the Criminal Code makes it an offence for a public official to disclose confidential information. Additionally, Section 83 makes it an offence to use such information for personal gain or to cause detriment to another person.

Section 30 of the *Regional Development Commissions Act 1993* makes it an offence to disclose confidential information, either directly or indirectly, except in the performance of a function covered by the Act.

Some government information, both paper and electronic, is available for access by the public and this access should be encouraged. Other information is considered Official Information and should not be released.

DPIRD's Privacy Policy will be referred to should any matters arise, that may not be addressed within this policy.

Definitions

Personal Information: means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material (or digital) form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Official Information: means information, whether in a record or not, that comes to the knowledge of, or into the possession of, a person because the person is a public servant or government contractor.

Policy

1. The Commission is committed to safeguarding the Personal Information it may hold at any time in respect to an individual.
2. All Commission staff must familiarise themselves with the IPPs Guidelines which provide detailed explanations of the IPPs, including the specific exceptions and departures as well as consequences of failure to comply.
3. The Commission will:
    a. Handle personal information lawfully by collecting, using, disclosing, or otherwise handling personal or de-identified information in a manner consistent with the Information Privacy Principles set out in Schedule 1 of the PRIS Act.
    b. Only collect information which is required for a specified primary purpose.

c. not use or disclose Personal Information about an individual for a purpose other than:

   i. the purpose for which it was collected;

   ii. a related purpose (or in the case of sensitive information, a “directly related” purpose) which the individual would reasonably expect;

   iii. a purpose required or permitted by law; or

   iv. any alternative purpose for which the consent of the individual has been obtained.

d. take all reasonable steps to make sure that the Personal Information collected, used or disclosed is accurate and up to date

e. take all reasonable steps to protect and safeguard that Personal Information collected is destroyed when it is no longer required for the purpose for which it was collected

f. make available policies relating to the management of Personal Information

g. provide people with access to their own Personal Information and permit people to seek corrections if necessary.

h. respond to suspected notifiable information breaches by taking appropriate steps to assess, contain, and mitigate a suspected unauthorised access, disclosure, or loss of personal information

i. notify affected individuals and the Information Commissioner in a timely manner should a serious information breach occur.

j. follow compliance directives from the Information Commissioner in response to a suspected notifiable information breach

k. conduct a privacy impact assessment in high-impact privacy activities (involving the collection, use, or disclosure of personal information with a significant potential impact on privacy), or when directed by the Information Commissioner

l. ensure that personal information held in public registers that the department is legally responsible to maintain is properly safeguarded

and remove or protect such information when it affects an individual's safety or wellbeing.

Collection of Personal Information

4. The Commission will not ordinarily collect any information about an individual except where it is provided by the individual for the purposes of undertaking regional development activities.

5. Personal Information may need to be collected from third parties in the course of carrying out the Commission's responsibilities, ensuring that the information provided is correct. Third parties acting on behalf of the Commission will also be subject to the PRIS Act privacy obligations if stipulated in their contract.

6. Prior to collecting personal information, the Commission will inform individuals via a Collection Notice outlining the reasons for collection, how the Commission will use the information collected, any consequences if the information is not provided and who might the Commission share the information with.

7. The type of Personal Information the Commission may collect includes name, address, telephone number and e-mail address. In addition, the system used to pay accounts may also record bank account details to enable payment by the electronic transfer of funds.

8. Personal Information is normally collected to facilitate contact with individuals and organisations. Personal Information collected may be:

    - Factual or routine information (such as address, date of birth, length of employment and names of dependents)
    - Sensitive (such as, religious beliefs, health status or ethnic origins)
    - Interpretative, including opinions or evaluative material such as advice or recommendations of a third party (such as records of interviews and medical reports) and information in personnel records and business systems.

9. Personal Information may be collected in person, in writing (including email), by telephone, through the Commission's websites and other methods of communication with individuals.

Use of Information

10. The Commission will take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure. In circumstances where required, the Commission will destroy or de-identify personal information.
11. The Commission will not make use of Personal Information which it has collected except for the purpose for which it was collected, or for a purpose reasonably expected in carrying out regional development activities, including the evaluation of services, for contacting clients or partners, or for paying accounts.
12. Employees and Board members must not use Official Information for their personal or commercial gain or that of work colleagues or associates. This includes speculation in shares based on confidential information or disclosing the contents of any official papers to unauthorised persons.

Disclosure of Information

13. Personal Information may be disclosed to third parties to which it is reasonable to expect that information would be provided in the course of, or incidental to the Commission carrying out its statutory responsibilities.
14. The Commission will not disclose Personal Information not already available to the public at large, to another person, unless consented to by the individual or to assist in the recovery of Commission property.
15. Personal Information must be kept confidential and must not be released without the permission of the individual concerned unless required by law to do so.
16. Official Information can only be disclosed with the express permission of the Chief Executive Officer (CEO), by an officer with delegated authority from the CEO, by the custodian of the official information (if external to the Commission) or if it is required to be disclosed in the course of official duties.
17. Employees and Board members must not discuss or release information concerning the Commission's customers to any unauthorised persons, other Commission staff or other Government departments unless it is necessary and proper for them to do so in the normal course of their duties.

18. Unless authorised to do so, employees and Board members must not:

    a. give to any person any Official Information related to the business of the Commission, the public service or the Government which has been obtained in the course of their work
    b. disclose the contents of any official papers, documents or files.

Access to Information

19. The Commission will take reasonable steps to protect Personal Information from misuse and loss, and from unauthorised access, modification or disclosure. When information is no longer needed, reasonable steps will be taken to destroy or permanently de-identify any Personal Information.

20. Information held by the Commission will be treated in a manner consistent with the requirements of the *Freedom of Information Act 1992*, in that information that has not been classified as protected can be available to the public.

21. Requests from an individual to review the Personal Information held about them by the Commission should be made in writing to the CEO.

22. If requested, Personal Information will be made available to that same individual, except where:

    a. it would have an unreasonable impact on the privacy of others
    b. the information relates to legal proceedings with the individual requesting access
    c. the information would reveal Official Information, or a commercially sensitive decision-making process
    d. providing access to the information would prejudice certain investigations
    e. the Commission is required by law not to disclose the information.

Correcting Inaccurate Information

23. The Commission will take reasonable steps to ensure that Personal Information is accurate, complete and up to date. Individuals may ask to see their personal details to ensure that they are correct and ask to have incorrect data changed.

24. If an individual believes that their Personal Information is inaccurate, incomplete, out of date or misleading they can apply to the CEO to have it amended or destroyed. The CEO, or an authorised delegate, will review and update the relevant information as necessary.

Complaints

25. Any complaints about how the Commission has handled Personal Information must be made in writing to the CEO, who will carry out a review in accordance with the legislation referred to in the Introduction section of this policy and processes specified in the Commission's Freedom of Information Statement.

26. The Peel Development Commission website records and logs the following information for statistical purposes:

- the user's server address
- the user's top level domain name (e.g. .com, .gov, .au, .uk etc.)
- the date and time of the visit to the site
- the pages accessed and documents downloaded
- the previous site visited
- the type of browser used.

No attempt will be made to identify users or their browsing activities except, in the unlikely event of an investigation, where a law enforcement agency may exercise a warrant to inspect the service provider's logs.

Who does the Policy apply to?

The policy applies to Board members, all employees resourced to the Commission regardless of classification or level, full time or part-time status, whether paid or unpaid, on permanent or on fixed term contracts, as well as trainees, work experience placements, volunteers and contractors working for the Commission.

Roles and Responsibilities

All Staff:

1. Comply with this Privacy Policy and applicable privacy legislation.

2. Proactively support privacy and responsibly share information while administering ongoing duties and work activities.
3. Report any issues/concerns with management of personal information.
4. Complete DPIRD's privacy training on Progi.
5. Use department-approved systems and tools to manage personal information.
6. Avoid using personal devices or unofficial channels for work-related activities involving personal information.
7. Must refrain from:
    a. Accessing personal information for personal or unauthorised purpose
    b. Forwarding personal information via unsecured communication channels
    c. Posing unnecessary risks of personal information breaches by reckless or irresponsible behaviour, e.g., sharing passwords or leaving systems unattended.

CEO, Director and Line Managers

8. Lead by example in applying the IPPs in their teams.
9. Ensure staff are trained and comply with privacy obligations.
10. Manage personal information within their areas in accordance with policy.
11. Monitor compliance with the IPPs. Identify issues/concerns with management of personal information.

Commission PRIS Coordinator (SAO):

12. Promote, manage, implement and monitor the Commission's compliance with the PRIS Act.
13. Support Commission staff and external stakeholders seeking advice on privacy management practices.
14. Coordinate the Commission's dealings with DPIRD and the Information Commissioner as required.
15. Ensure alignment with Freedom of Information (FOI) procedures where applicable in response to requests to access or correct personal information.
16. Support the Commission's information breach response and notification as required.
17. Liaise with the Commission's Communications Advisor in regard to formal external PRIS correspondence.

18. Monitor updates from DPIRD and/or the Office of the Information Commissioner.