Department of **Biodiversity, Conservation and Attractions**

GOVERNMENT OF WESTERN AUSTRALIA

CORPORATE POLICY STATEMENT NO. 29

PRIVACY OF PERSONAL INFORMATION

December 2025

1. OBJECTIVE

To provide direction on how personal information is to be handled by the Department of Biodiversity, Conservation and Attractions (the department), as required by the *Privacy and Responsible Information Sharing Act 2024*[1] (PRIS Act).

2. SCOPE

This policy applies to personal information the department handles as part of its functions, unless otherwise covered by another specific key document. This policy applies to all employees of the department, including the statutory authorities of the Botanic Gardens and Parks Authority, Rottnest Island Authority and Zoological Parks Authority, and any volunteers involved in the handling of personal information. It outlines obligations that employees have in handling personal information according to the requirements of the PRIS Act.

This policy does not cover:

- The handling of personal information belonging to the department's employees and volunteers.
- The handling of personal information that is publicly available, as defined in section 22 of the PRIS Act.
- The responsible information sharing of government information. Refer to Part 3 of the PRIS Act.
- The handling of sensitive Aboriginal traditional information. A specific Cultural Knowledge Protocol is being developed by the Parks and Visitor Services Division to address this.
- Information security management. Refer to Corporate Policy Statement No. 70: Information Security Management for guidance on how personal information is protected by the department.
- How personal information and related matters will be handled in the event of an information breach. A specific information breach policy, response plan and register are being developed to address this.

3. CONTEXT

The PRIS Act provides a framework that protects personal information held by public entities. It introduces 11 Information Privacy Principles (IPPs) that govern the handling and security of personal information, which must be met by the department and other government agencies.

[1] The PRIS Act received Royal Assent on 6 December 2024. Parts 1 and 7 and Part 2, Division 12, are in effect with the majority of Parts 2 and 3 (privacy and responsible information sharing provisions) anticipated to come into force on 1 July 2026, and the notifiable information breach provisions anticipated on 1 January 2027.

The State's Information Commissioner, supported by the Privacy Deputy Commissioner and Information Access Deputy Commissioner, will oversee privacy matters and freedom of information under the *Freedom of Information Act 1992* (FOI Act). These officials are independent and report directly to Parliament. The Chief Data Officer will oversee government information sharing under the PRIS Act and sits within the Department of the Premier and Cabinet.

Personal information is information or an opinion that relates to an individual, that may directly or indirectly be used to identify that person. The department handles a significant amount of personal information as part of its many statutory functions, including licence applications, accommodation reservations, research, provision of services and facilities, administering programs and grants, compliance and enforcement.

The types of personal information that may be handled by the department are as follows:

- a name, date of birth or address;
- a unique ID, online ID or username;
- contact information;
- information that relates to a person's location;
- technical or behavioural information in relation to a person's activities, preferences or identity;
- inferred information, including predictions on a person's behaviour (e.g. for investigations of non-compliance);
- identity-related information (e.g. physical, mental, economic or cultural identity); and
- sensitive personal information (e.g. racial or ethnic origin, gender identity, criminal history, health information); and
- images in photographs or video (in which a person's identity is clear or can reasonably be ascertained from that image).

This policy is a requirement of IPP 5 of the PRIS Act, which provides for 'Openness and Transparency' and requires that each public entity develop a policy on how personal information is handled.

4. LEGISLATION

This policy is consistent with, and will operate within any applicable legislative, policy and strategic frameworks. This includes, but is not limited to:

Legislation:

- *Biodiversity Conservation Act 2016;*
- *Botanic Gardens and Parks Authority Act 1998;*
- *Conservation and Land Management Act 1984;*
- *Freedom of Information Act 1992;*
- *Information Commissioner Act 2024;*
- *Privacy Act 1988 (Commonwealth);*
- PRIS Act;
- *Public Sector Management Act 1994;*
- *Rottnest Island Authority Act 1987;*
- *State Records Act 2000;*
- *Swan and Canning Rivers Management Act 2006;*
- *Zoological Parks Authority Act 2001.*

Policy and strategic frameworks:

- Western Australian Information Classification Policy;
- Western Australian Open Data Policy;
- Western Australian Government Cyber Security Policy 2024;
- Digital Strategy for the Western Australian Government 2021-2025;
- Corporate Policy Statement No. 63 – Information and Related Technology;
- Corporate Policy Statement No. 7 – Information Quality Management;
- Operational Procedure – Information Quality Management Framework;
- Corporate Policy Statement No. 70 – Information Security Management;
- the department's Digital and IT Strategy;
- DBCA Enterprise Architecture Framework for IT.

5. DEFINITIONS / GLOSSARY / ACRONYMS

Automated decision-making process	a process under which a decision the department is responsible for is made, or significantly influenced, by an automated electronic system, including a computer information-processing system or an artificial intelligence system.
Collection notice	a statement provided to an individual notifying them that personal information is being collected and outlining how it will be handled.
Cookies	cookies are blocks of data that are shared between a web server and the user's (the person accessing the website) browser (the application used by the person to browse the internet).
De-identify	means to modify personal information so that the identity of the person is no longer apparent.
Department	Department of Biodiversity, Conservation and Attractions.
Government information	in relation to a public entity means the information (including personal information) held by the public entity; but does not include any exempt information held by the public entity.
Handle	in relation to personal information, means to collect, hold, manage, use or disclose the information.
Identity-related information	information that relates to a person's physical, physiological, genetic, mental, behavioural, economic, cultural or social identity (e.g. information that allows the department to determine whether a person identifies as Aboriginal, has a disability, or may speak a language other than English).
IPP	Information Privacy Principles
Personal information	means information or an opinion that relates to a person that may directly or indirectly be used to identify that person, including a name, date of birth or address; a unique ID, online ID or username; contact information; location information; technical or behavioural information, identity-related information; and sensitive personal information.
PRIS Act	*Privacy and Responsible Information Sharing Act 2024*.

Privacy Impact Assessment	an assessment of a function or activity to determine: the likelihood that it will interfere with a person's privacy; the impact it may have on a person's privacy; and recommendations for managing, minimising or eliminating that impact.
Public entity	means any department, entity, body, or holder of office (to be prescribed by regulations) included in section 6 of the PRIS Act.
Sensitive Aboriginal traditional information	means information that should not be disclosed to people who are not knowledge holders of that information.
Sensitive personal information	means personal information that relates to, or can lead anyone to reasonably infer, a person's racial or ethnic origin, gender identity, sexual orientation, political opinions, religious beliefs or affiliations, membership of a professional or trade association or union, criminal record, health information, genetic or genomic information, biometric information.
Unique ID, online ID or username	a unique identifier assigned by a system or chosen by a person for their personal account, user information or check-out details held with the department that may link back to personal information (e.g. registration details, customer number, licence or permit number).

6. POLICY

6.1 The department will enable individuals to interact anonymously with the department, where possible (for example, making a complaint).

6.2 The department will take all reasonable steps to ensure that any personal information that is handled is accurate, complete, up-to-date and relevant.

6.3 The department must provide access to an individual's personal information if requested and take reasonable steps to correct that information if required. Requests to access or correct personal information should be directed to privacy@dbca.wa.gov.au.

Collection of personal information

6.4 The department will only collect personal information necessary for, or directly related to its functions or activities, including: for the purposes of biodiversity conservation, managing the land and waters it has responsibility for, providing advice to other agencies, provision of services and facilities, administering programs and grants, research, assessing applications, processing payments, compliance and enforcement, preparing for or responding to incidents. This may extend to personalising products and services provided by the department or administering a promotion or survey to attract visitors or improve experiences.

6.5 Personal information may be collected from a person directly or indirectly through an authorised representative of the department or via a third party (for example, a third party engaged to facilitate public consultation, or a booking agent or tourist information centre). This information may be collected verbally (in-person or over the phone), in writing or via forms, contracts or agreements, digital applications or surveys (in-person or online).

6.6 Personal information is generally provided to the department knowingly and voluntarily, unless:

- in the event of a suspected offence under the department's legislation, the person is lawfully directed to provide personal information by an authorised officer; or
- in the event of an incident or emergency, personal information is provided to the department from a separate person or third party who reported the incident; or
- the information was provided to the department by another agency or organisation; or
- a person is accessing the department's websites, in which case their IP address and top level domain name (e.g. .com, .au, .gov), date and the time of visit to the site, pages accessed and documents downloaded, time spent on pages, address of the last site visited, unique device identifiers, operating system and type of browser used, is automatically collected.

6.7 When personal information is being collected by the department, it must be clear and apparent to the individual that their information is being collected (for example, through collection notices).

6.8 The department must keep a written record of the purpose(s) for which personal information is collected and used or disclosed (for example, through collection notices).

Purpose for collecting personal information

6.9 The department may collect personal information for the purpose of undertaking its functions or activities, including marketing or promotional purposes.

6.10 The department's purpose for collecting personal information should be clear and apparent to the person providing the information (for example, a person's name, address and date of birth may be collected to create a unique account on the department's Park Stay WA campground booking system to secure a campsite and confirm that the person is at least 18 years old).

6.11 When a person visits any of the department's websites, their IP address and top level domain name (e.g. .com, .au, .gov), date and the time of visit to the site, pages accessed and documents downloaded, time spent on pages, address of the last site visited, unique device identifiers, operating system and type of browser used, is automatically collected for statistical, analytical and administration purposes as well as cyber safety and security purposes.

6.12 The department may use the information collected through cookies, image analytics, location data and similar technology, for the purpose of continually improving the functionality and efficiency of its websites and to refine content served through some marketing campaigns.

6.13 The department may collect personal information for the purposes of creating an account for various software, systems or applications to enable an individual to access its services; obtain a Parks Pass, membership or subscription; apply for an approval or grant; to process a payment; or other services or functions carried out by the department that require an account.

6.14 The department may collect identity-related information for the purpose of ensuring that the services it provides and land and facilities it manages is inclusive and accessible to all people.

6.15 The department may explicitly request sensitive personal information if it is relevant to any of its functions or activities and is in the public interest (for example, to obtain a fauna-related licence, the applicant is required to disclose any convictions for wildlife-related offences in the past five years).

Holding, management and use of personal information

6.16 The department will take all reasonable steps to protect personal information from misuse, loss, and unauthorised access, modification or disclosure.

6.17 The department may hold personal information in non-digital (hardcopy files) or digital format in systems or applications developed within the department or in trusted third-party systems or applications licensed to the department (for example, Microsoft products, recordkeeping systems, and financial management systems).

6.18 Personal information must be stored securely and managed in accordance with Corporate Policy Statement No. 7 - Information Quality Management, Operational Procedure - Information Quality Management Framework, Corporate Policy Statement No. 70 – Information Security Management; and the department's Recordkeeping Plans.

6.19 Any systems within the department that store personal information outside of Australia must meet the standards set out in the WA Government Cyber Security Policy.

6.20 Personal information must be used in accordance with the purpose stated unless the alternative purpose complies with clause 6.21.

6.21 Personal information may be used by the department for an alternative purpose if:

- it is a reasonable extension of the purpose stated; or
- the owner of the personal information has consented, in writing, to an alternative use; or
- the department reasonably believes it is necessary to prevent or lessen a serious threat to the life, health, safety or welfare of any individual, public health, public safety or public welfare or a threat to any individual due to family violence; or
- required or authorised by law or court/tribunal order; or
- required to investigate or report suspected unlawful activity, or when reasonably necessary for a specified enforcement purpose; or
- it is necessary for research, or the compilation or analysis of statistics, in the public interest and the outcome is not published in a form that would identify any person.

6.22 The department will take reasonable steps to lawfully destroy or permanently de-identify personal information if it is no longer needed (unless required or authorised by law to retain or reinstate the personal information).

6.23 Personal information that has been de-identified will be securely handled and/or destroyed in accordance with Corporate Policy Statement No. 7 - Information Quality Management, Operational Procedure - Information Quality Management Framework, Corporate Policy Statement No. 70 – Information Security Management; and the department's Recordkeeping Plans.

Disclosing personal information

6.24 The department may disclose personal information to another public entity or third party if:

- the disclosure of the information is related to the collection purpose stated and the owner of that personal information was informed (or would reasonably expect) that it may be disclosed; or
- the owner of the personal information has consented, in writing, to its disclosure; or

- the department reasonably believes it is necessary to prevent or lessen a serious threat to the life, health, safety or welfare of any individual, public health, public safety or public welfare or a threat to any individual due to family violence; or
- required or authorised by law or court/tribunal order, including under the information sharing provisions of the FOI Act, PRIS Act or *Biodiversity Conservation Act 2016*; or
- required to investigate or report suspected unlawful activity, or when reasonably necessary for a specified enforcement purpose; or
- it is necessary for research, or the compilation or analysis of statistics, in the public interest and the outcome is not published in a form that would identify any person.

6.25 The disclosure of personal information will be undertaken in an appropriate and secure way.

6.26 Instances where personal information has been disclosed by the department should be recorded in writing, including what personal information was disclosed, to whom and for what purpose. Records must be kept in accordance with the department's recordkeeping requirements.

6.27 Before personal information is disclosed, the department should take all reasonable steps to confirm that the recipient has the appropriate technical and physical controls in place to keep information secure.

Other

6.28 The department will not implement any automated decision-making processes that involve the use of personal information. All decisions, including those that utilise an automated electronic system to some capacity (including a computer information-processing system or an artificial intelligence system), will be subject to human review and intervention.

6.29 Systems and software used by the department may assign unique identifiers that are tied to a person's personal information in order to manage a significant amount of data or assist in compliance (examples include, licence or permit numbers, customer numbers, user IDs, etc.).

6.30 The department may collect a person's technical or behavioural information through its systems, software or surveys in order to inform future products or services, events, policy or strategic decisions (for example, determining the most popular camp sites managed by the department).

6.31 The department will undertake a Privacy Impact Assessment before performing a new activity, or making a significant change to an existing activity, where it involves the handling of personal information and is likely to have significant privacy implications.

7. STANDARDS

The following documents provide direction and standards, including expectations regarding employee behaviour in relation to this policy:

- PRIS Act;
- WA Government PRIS Readiness Plan and supporting Readiness Guidance documents (including the Readiness Checklist); and
- DBCA's Code of Conduct.

8. POLICY IMPLEMENTATION STRATEGIES

The department will:

8.1 Review and update privacy-related content on the department's websites to align with this policy and incoming changes under the PRIS Act.

8.2 Develop a Privacy Impact Assessment template and guidance.

8.3 Ensure this policy is supported by an information breach policy, response plan and breach register.

8.4 Identify and develop suitable training and awareness activities.

8.5 Develop and publish collection notices where required.

8.6 Ensure contracts with partners and service providers have suitable arrangements for handling personal information, where required.

8.7 Ensure internal retention and disposal processes that relate to personal information held by the department are compliant with the PRIS Act.

8.8 Establish internal procedures for handling and tracking PRIS requests, complaints or breaches.

8.9 Establish and maintain a register of all systems storing personal information to support the implementation of this policy.

9. CUSTODIAN

Deputy Director General Science, Strategy and Governance.

10. PUBLICATION

This policy will be made available on the department's intranet and website and must be provided to any person on request.

11. KEY WORDS

Personal information, sensitive personal information, privacy, disclosure.

12. REVIEW

This policy will be reviewed when the full provisions of the PRIS Act commence in 2027.

13. APPROVAL

Approved by

Stuart Smith
DIRECTOR GENERAL
CHIEF EXECUTIVE OFFICER

Date: 19 December 2025