



Privacy Policy

Purpose

This Policy explains how the Office of the Chief Psychiatrist (OCP), a public authority of the Government of Western Australia, collects, uses, discloses and protects personal information. It sets out how to access and correct your personal information.

In addition to its obligations under this Privacy Policy, OCP is subject to a number of legal requirements that affect how it collects, uses and discloses personal information. Those legal requirements include legislative frameworks including the *Privacy and Responsible Information Sharing Act 2024 (WA)* (Pris Act), the *Freedom of Information Act 1992 (WA)* (FOI ACT) and the *State Records Act 2000 (WA)*.

The Department's Role

The OCP is an independent statutory office established under the *Mental Health Act 2014 (WA)*. The Chief Psychiatrist exercises powers and functions that provide governance and oversight of the treatment and care provided by mental health services in Western Australia.

If you have been directed to this page, that means the OCP may be collecting your data when carrying out its functions and role. Click [here](#) to see how OCP deals with your data in accordance with Western Australian law.

The OCP is considered an IPP 'entity' under the PRIS Act, which means the OCP must comply with the Information Privacy Principles (IPPs) established under the PRIS Act from 1 July 2026. The OCP will only collect information lawfully, fairly and reasonably in line with the IPPs.

Policy Principles

1. Scope

This policy applies to:

--

- All OCP employees and contractors, and third-party service providers.
- All OCP information held by the OCP, contractors and other organisations that have received OCP information under agreement or contract.
- All types and formats of information, including personal and non-personal information.
- All systems, including digital platforms, records systems, surveillance systems, and third-party hosted environments.
- All websites operated by the OCP.
- All interactions with members of the public, service providers, and partner agencies.

This Policy is supported by public-facing privacy statements applicable to specific services and channels (e.g. websites).

2. Legislative and Policy Framework

The OCP manages personal information in accordance with:

- The *Privacy and Responsible Information Sharing Act 2024 (WA)* (Pris Act)
- Applicable Information Privacy Principles (IPPs)
- *Mental Health Act 2014 (WA)*
- *Freedom of Information Act 1992 (WA)*
- *State Records Act 2000 (WA)*
- Applicable whole-of-government policies and standards
- [OCP's Privacy Statement 2026](#)

3. Information Privacy Principles

The OCP is committed to implementing and maintaining practices, procedures, and systems to ensure compliance with the IPPs, including:

- Lawful and fair collection
- Purpose limitation
- Data quality and security
- Transparency
- Access and correction rights

4. Collection of Personal Information

The OCP only collects personal information for purposes reasonably necessary for, or directly related to, one or more of its functions or activities, or when the information is knowingly or voluntarily provided by an individual.

Methods of collection include:

- Forms (online and paper-based)
- Correspondence (email, phone, in person)
- Website interactions and registrations
- Surveys and consultations
- Applications, bookings and service requests
- Financial transactions
- CCTV and body-worn camera recordings
- Site access and inductions
- Agreements and licensing arrangements

Personal information may also be collected from:

- Publicly available sources
- Other government agencies
- Third parties where authorised or permitted

Types of personal information include:

- A person's name, address and contact details;
- Information about a person's identity (e.g. date of birth, passport details, drivers' licence, birth certificates, ATM cards, portrait photograph);
- Gender and marital status;
- Concession details;
- Cardholder data;
- Bank account details;
- Public interest disclosure applications;
- Criminal history and working with children checks;
- Employment details (including work history, referee comments and remuneration) and employee health details;
- Occupation details;

- Insurance details;
- Educational qualifications;
- Government identifiers (e.g. Tax File Number);
- Security incident details;
- Financial position, organisation details and credit check information;
- Telephone and audio recordings;
- CCTV video surveillance recordings;
- Body camera images and recordings;
- Social media posts; and
- Content of email messages and email addresses of the sender and recipients.

How information is collected:

The OCP will provide a collection statement whenever it is collecting personal information detailing what is being collected, and how the information is used and shared. For example, if an individual submits an online form for contact, subscribes to receive newsletters, signs up for a promotion, or offers services, the OCP will ask the individual to provide their name and contact details.

Providing the requested information is voluntary. If individuals choose not to provide the OCP with the requested information, the OCP may not be able to respond to the individual or provide the services the individual is seeking.

5. Collection Notices

The OCP will issue collection notices when collecting personal information as part of its commitment to openness, transparency, and privacy-by-design. Individuals will be made aware of how personal information will be handled at or before collection, including being provided with the following information:

- Purpose of collection;
- Authority to collect the information;
- Consequences of not providing the information; and
- Rights of access or correction.

6. Use of Personal Information

Use of personal information for the express or implied purpose provided

The OCP uses personal information for the purposes described in the collection statement. The OCP may also use information for a purpose related to the purpose for which it was collected, if it is reasonably expected the personal information would be used for that related purpose.

The OCP uses personal information primarily for:

- Performing statutory and regulatory functions
- Delivering and administering services
- Managing stakeholder relationships
- Responding to enquiries, complaints and feedback
- Research, planning, and policy development
- Ensuring safety, security, and compliance

7. Disclosure of Personal Information

The OCP may use or disclose personal information to third parties where it is legally required to do so, such as where required or permitted by a law of Western Australia (e.g. under the *Freedom of Information Act 1992 (WA)*), and/or if required by law to do so (e.g. by a court or tribunal order, or a law of the Commonwealth). Personal information will at all times be dealt with in accordance with the applicable legislation in Western Australia.

The OCP will only disclose personal information where:

- It is for the primary purpose of collection
- It is for a permitted secondary purpose; or
- It is required or authorised by law

Permitted disclosures include to:

- Other WA government agencies and Ministers
- Mental health system partners (e.g. Mental Health Commission, Tribunal, Department of Health)
- Contractors and service providers
- Law enforcement and regulatory bodies
- Auditors, insurers, and legal advisers
- Emergency services
- Entities engaged in research, investigation, or fraud prevention.

Specific use – Surveillance data:

CCTV and body camera recordings are used and disclosed to:

- Maintain safety and security
- Investigate incidents
- Support enforcement and legal proceedings

8. Information Sharing

Where information sharing is permitted, the OCP will adhere to the “Responsible sharing principles’ established under the PRIS Act.

Personal information may be disclosed in special situations where the OCP has reason to believe that doing so is necessary to identify, contact or bring legal action against anyone damaging, injuring, or interfering (intentionally or unintentionally) with its rights or property, users, or anyone else who could be harmed by such activities.

All information sharing will be:

- Lawful and proportionate
- For a defined purpose
- Subject to appropriate governance, agreements, and safeguards

9. Data Quality

The OCP takes reasonable steps to ensure personal information is:

- Accurate
- Complete
- Up-to-date
- Relevant for its intended use

10. Data Security

The OCP takes all reasonable steps to implement the appropriate security policies, rules, measures and security patches to protect the personal information that it has under its control from:

- Misuse
- Interference and loss
- Unauthorised access, modification, or disclosure

These include:

- Secure ICT systems
- Access controls
- Monitoring and logging
- Cybersecurity protections

11. Retention and Disposal

Personal information is retained and disposed of in accordance with:

- *State Records Act 2000 (WA)*
- Approved retention and disposal schedules

The OCP will take reasonable steps to:

- Destroy or de-identify personal information when no longer required.

12. Access and Correction

Individuals have a right to request access to personal information that the OCP holds under both the FOI Act and the PRIS Act. Individuals can apply to have their personal information corrected if the information is inaccurate, incomplete, out of date or misleading.

The OCP will manage any requests for access to personal information and for correction of personal information in accordance with the terms of the FOI Act. Information about how to apply can be found on the OCP website.

13. Direct Marketing

The OCP may use personal information to communicate information about its services, initiatives, or updates. This may also be undertaken through its media service providers.

Individuals will be provided with:

- A clear ability to opt out; and
- The ability to withdraw consent at any time.

14. Overseas Disclosure

The OCP will not disclose personal information to overseas third parties unless permitted to do so under the PRIS Act, or consent has been obtained for the disclosure.

Where this occurs, the OCP will take reasonable steps to ensure:

- Appropriate safeguards are in place
- Handling is consistent with applicable privacy requirements.

15. Website, Cookies and Digital Services

The OCP website may collect statistical and usage information through cookies and analytics tools to:

- Improve user experience
- Support service delivery

Users may disable cookies, though functionality may be impacted.

When following a link from the OCP website and it takes you to a third-party website, the OCP recommends that you read the Privacy Policy of that other website to understand how that third-party website deals with your information. The OCP is not responsible for any content, privacy policies, or privacy practices of any third-party websites that may be linked to from the OCP website.

16. Incidental Access by Contractors

Information will only be accessed by OCP staff to carry out the functions of the Chief Psychiatrist or provide related services. Information may be shared with the OCP's contractors, project partner, or suppliers responsible for carrying out the OCP's functions and services. All service providers are required to comply with Australian Privacy Laws as applicable and, where appropriate, are required to enter into privacy agreements with the OCP to ensure they are bound by the PRIS Act.

17. Social Media

The OCP uses third-party platforms (e.g. LinkedIn, YouTube) to engage with the public. Users should be aware:

- These platforms operate under their own privacy policies
- Information may be stored or processed outside of Australia.

The OCP may collect and use information from these platforms for engagement, recordkeeping, communications and campaigns.

18. De-identified information

The OCP will take reasonable steps to protect the de-identified information it holds from misuse and loss from unauthorised re-identification, access, modification or disclosure. The OCP will only re-identify data in a manner that is consistent with the IPPs.

19. Information Breach Management

The OCP maintains processes to identify, assess, and respond to data breaches. This includes:

- Containment and mitigation
- Risks assessment
- Notification (where required under PRIS requirements)

20. Notifiable Breaches

The OCP maintains information breach response procedures in relation to information breaches. From 1 January 2027, where an information breach is likely to result in serious

harm, the OCP will notify the Information Commissioner and affected individuals in accordance with the PRIS Act. Until that date, the OCP continues to meet any other applicable notification duties.

21. Roles and Responsibilities

Role	Responsibility
Chief Psychiatrist	Responsible for the overall accountability for privacy governance.
Business Units	Responsible for lawful collection and use.
All Staff (and Third Party or Service Providers)	Responsible for compliance with this Policy and applicable procedures.

22. Complaints and Enquiries

Individuals may contact the OCP to:

- Make a privacy complaint
- Raise concerns about handling of personal information

Complaints will be handled in accordance with applicable legislation and may be escalated to the Information Commissioner.

The PRIS Act establishes a complaints regime that includes a procedure for dealing with complaints, a process for resolution or conciliation, and powers for the Information Commissioner to deal with unresolved complaints.

23. Relationship to Privacy Statements

This Policy is supported by public-facing privacy statements that provide more specific information about how personal information is handled in particular contexts (e.g. website interactions).

24. Review and Updates

This Policy will be reviewed periodically and updated to ensure alignment with legislative changes, whole-of-government requirements and emerging privacy risks and practices.

Definitions

The following definitions are relevant to this Policy.

Term	Definition
------	------------

Direct marketing	Involves the use and/or disclosure of personal information to communicate directly with an individual to promote goods and services. A direct marketer may communicate with an individual through a variety of channels, including telephone, SMS, postal mail, email and online advertising.
Personal information	Has the meaning given in the PRIS Act: (a) information or an opinion, whether true or not, and whether recorded in a material form or not, that relates to an individual, whether living or dead, whose identity is apparent or can reasonably be ascertained from the information or opinion; and (b) includes information of the following kinds to which paragraph (a) applies – (i) a name, date of birth or address; (ii) a unique identifier, online identifier or pseudonym; (iii) contact information; (iv) information that relates to an individual's location; (v) technical or behavioural information in relation to an individual's activities, preferences or identity; (vi) inferred information that relates to an individual, including predictions in relation to an individual's behaviour or preferences and profiles generated from aggregated information; or information that relates to 1 or more features specific to the physical, physiological, genetic, mental, behavioural, economic, cultural or social identity of an individual.
Primary purpose	Refers to the particular purpose for which the information in question was collected.
Sensitive information	Is a subset of personal information, including information relating to an individual's racial or ethnic origin, gender identity, sexual orientation, membership in political associations, religious or philosophical beliefs, membership in professional or trade associations, trade union membership, or criminal record. Includes information relating to health, mental health, criminal history, or other categories as defined under applicable privacy laws.
Secondary purpose	Is any purpose other than the primary purpose for which we have collected your personal information.

Related Documents

The following documents are mandatory pursuant to this Policy:

- Privacy Act 1988 (Cth)
- *Privacy and Responsible Information Sharing Act 2024* (PRIS Act)
- OCP Privacy Statement 2026
- State Records Act 2000
- OCP Record Keeping Procedures 2025

- Information Breach Policy
- Information Breach Response Plan

Policy Contact

Enquiries relating to this Policy may be directed to:

Title: Director Corporate and Clinical Governance
 Directorate: Corporate and Clinical Governance
 Email: creswell.surrao@ocp.wa.gov.au

Document Control

Version	Published date	Effective from	Review date	Effective to*	Amendment (s)
0.1	18/03/2026				First Draft
1.0	30/06/2026				Final Version

* 'Effective to' dates must only be displayed when the mandatory policy is initially published if it is intended that the mandatory policy will cease to be in effect on that day. Otherwise, this column will be used to record the date a Mandatory Policy ceases to be in effect following the release of a new version of the Mandatory Policy. When the version remains in effect the column will display as 'current'.

Approval

Approval by	Director Corporate and Clinical Governance
Approval date	30 June 2026

Acknowledgement

This policy template is based on the template developed by the Department of Health Western Australia, the Chief Psychiatrist acknowledges its use for consistency with thanks.

This document can be made available in alternative formats on request for a person with a disability.

© Office of the Chief Psychiatrist 2026

Copyright to this material is vested in the Office of the Chief Psychiatrist and the State of Western Australia unless otherwise indicated. Apart from any fair dealing for the purposes of private study, research, criticism or review, as permitted under the provisions of the *Copyright Act 1968*, no part may be reproduced or re-used for any purposes whatsoever without written permission of the State of Western Australia.