The independent regulator fostering trust and accountability in WA through privacy and freedom of information.

Guidance for IPP Entities

Resource 2: How PRIS applies to Contracted Service Providers

Office of the Information Commissioner
Western Australia

Publication date: 29/06/2026

Version Control: 01

Resource 2: How PRIS applies to Contracted Service Providers

Overview

Western Australian public sector entities must comply with the *Privacy and Responsible Information Sharing Act 2024* (WA) (PRIS Act), including the Information Privacy Principles (IPPs), when handling personal information. This extends to some third parties engaged under State services contracts and their sub-contractors (called contracted service providers or CSPs).

The purpose of this resource is to help WA public sector entities (referred to in this Resource as outsourcing entities) and CSPs understand their respective obligations when a CSP is engaged to provide services under a State services contract.

Managing the supply chain privacy risks is inherently challenging and is becoming more complex as core government business functions are increasingly outsourced. This is because the outsourcing entity sometimes has limited visibility into, and direct control of, the third-party's privacy practices. Nonetheless, the community expects their personal information will be afforded the same level of protection whether it is handled by a public entity or their CSPs.

Under the PRIS Act, outsourcing entities remain accountable for the way their CSPs handle personal information, unless the contract includes a provision which requires the CSP to comply with the privacy provisions of the PRIS Act (a PRIS compliance clause). When a contract includes a PRIS compliance clause, the CSP steps into the shoes of the outsourcing entity for the purposes of regulatory enforcement.

However, a PRIS compliance clause does not absolve the outsourcing entity from its responsibility to manage privacy risks associated with engaging a CSP. The outsourcing entity is responsible for:

- deciding what personal information the CSP will access
- undertaking appropriate due diligence
- ensuring the contract includes appropriate assurances
- ongoing monitoring to ensure the CSP is performing its obligations, and
- appropriate offboarding at the end of the contract.

An outsourcing entity should always work closely with its CSPs to ensure personal information is handled appropriately under a State services contract.

It is recommended this resource is read in full as it provides guidance for both outsourcing entities and CSPs. It should also be read in conjunction with IPP Summary, full text IPPs and Resource 1: Personal information collected before and after 1 July 2026 available on the Office of the Information Commissioner Western Australia's (OIC) website.

Key terms

Contracted service provider

A contracted service provider provides services to or on behalf of a public entity under a State services contract. It includes a person who is a subcontractor of a contracted service provider for the purposes of the State services contract (section 8 of the PRIS Act).

IPP entity

IPP entities are Western Australian Ministers, Parliamentary Secretaries, public entities and contracted service providers to government (section 14 of the PRIS Act).

Outsourcing entity

An outsourcing entity is a public entity who enters a State services contract with a contracted service provider (section 8 of the PRIS Act).

Public entity

A public entity includes Western Australian government departments, the WA Police Force, local and regional government, statutory authorities, public universities, government trading enterprises, and judicial bodies. It also includes bodies or office holders established for a public purpose under a written law or by the Governor or a Minister, or that is prescribed by regulations to be a public entity (section 6 of the PRIS Act).

PRIS compliance clause

A clause included in a State services contract which requires a CSP to comply with the IPPs and privacy provisions of the PRIS Act (see section 129 of the PRIS Act).

State services contract

A State services contract is a contract between a public entity (the outsourcing entity) and another person, who is not a public entity, under which services are provided to, or on behalf of, the outsourcing entity (section 8 of the PRIS Act).

The PRIS Act and State services contracts

The community expects their personal information to be afforded the same protection irrespective of whether it is handled by an outsourcing entity or a CSP acting on behalf of an outsourcing entity. The PRIS Act gives effect to this expectation by requiring outsourcing entities to take steps to ensure any personal information involved in an outsourcing arrangement is handled in accordance with the PRIS Act.

An outsourcing arrangement under a State services contract includes a CSP engaged to deliver a service or program on behalf of the outsourcing entity, or to provide services to the outsourcing entity to assist it to carry out its functions or activities.

Example 1 - Examples of services that may be provided under an outsourcing arrangement

- Information and communications services, such as websites, platforms and online portals
- Technology infrastructure and solutions, such as networking and data centre equipment, managed communications and infrastructure, cloud services and Software as a Service (SaaS)
- Community and social services
- Consultation and engagement with stakeholders
- Professional or consultant services such as audit or review services
- Interpreting and translating services
- Staff management services including recruitment, human resources and investigations
- Building security and maintenance services

Which party is accountable under the PRIS Act?

The PRIS Act provides two mechanisms to ensure CSPs handle personal information in accordance with the PRIS Act.

1. The State services contract includes a PRIS compliance clause requiring the CSP to comply with the privacy provisions in the PRIS Act and, as a result, the obligations apply to the CSP directly in relation to their handling of personal information under the contract (section 130 of the PRIS Act).
2. The outsourcing entity remains accountable under the PRIS Act for the actions of the CSP when it handles personal information under the contract (section 140 of the PRIS Act).

Whichever mechanism is adopted, the outsourcing entity remains accountable under the PRIS Act for its *own* handling of personal information in connection with the contract.

When is a CSP accountable under the PRIS Act?

PRIS compliance clause = CSP is accountable

Under the PRIS Act the CSP is accountable for how it handles personal information within the scope of the contract.

No PRIS compliance clause = outsourcing entity is accountable

Under the PRIS Act the outsourcing entity is accountable for the CSP's handling of personal information within the scope of the contract.

The contract includes a PRIS compliance clause

Section 129 of the PRIS Act provides when an outsourcing entity enters a State services contract it may include a contractual clause requiring the CSP to comply with the IPPs, the privacy provisions of the PRIS Act and any approved privacy code of practice (a PRIS compliance clause).

When a contract includes a PRIS compliance clause, the CSP must comply with the PRIS Act when handling personal information under the contract. If the CSP handles personal information inconsistently with the PRIS Act, the OIC may take regulatory enforcement action directly against the CSP under section 130 of the PRIS Act.

The CSP will not be required to comply with the PRIS Act in relation to personal information it handles outside of the contract. However, other privacy obligations, such as the *Privacy Act 1988* (Cth) or other contractual provisions, may apply to how the CSP handles personal information outside of the contract.

Importantly, the outsourcing entity will remain accountable for its own handling of personal information in connection with the contract, including the management of any third parties and the associated privacy risks.

Under the PRIS Act, a CSP includes a subcontractor (whether direct or indirect) of a CSP who is providing services on behalf of an outsourcing entity. When an outsourcing entity includes a PRIS compliance clause in a State services contract, it should consider requiring the CSP to flow down the clause to any subcontractors engaged for the purposes of the arrangement.

Example 2 – A PRIS compliance clause *is* included in the State services contract

A WA government department (the Department) enters a contract with a professional services company (the Company) to provide data migration services. The contract includes a PRIS compliance clause.

Under the contract, the Company was engaged to perform a platform transformation project which involved migrating the Department's employee information to a new payroll system. The Department provides the Company with access to the relevant employee personal information so it can perform the services under the contract. While performing the services, the Company is the target of a cyber-attack using log-in credentials stolen from a Company employee. A malicious third-party accesses and exfiltrates personal information relating to Department employees.

An employee of the Department makes a complaint to the Information Commissioner (Commissioner) in connection with the cyber-attack. Because the contract included a PRIS contract clause, the Commissioner can investigate the actions of the CSP, specifically whether it had taken reasonable steps to protect the personal information under IPP 4 and whether an unauthorised disclosure under IPP 2 has occurred.

Following the investigation, the Commissioner finds there was an unauthorised disclosure of personal information and the Company had failed to implement appropriate security controls to protect the information. The Company was required to pay compensation to the Department's employees.

In this example, the Commissioner may also investigate the actions of the Department. Specifically, whether the Department's failure to identify the security deficiencies during the procurement's due diligence phase amounted to a failure to take reasonable steps under IPP 4.

The outsourcing entity remains accountable for the actions of the CSP

Where the State services contract does *not* include a PRIS compliance clause, the outsourcing entity remains accountable for the CSP's handling of personal information under the contract.

Where the CSP (or its subcontractor) handles personal information inconsistently with the PRIS Act, enforcement action may be taken against the outsourcing entity as if it had engaged in the act or practice itself (rather than the CSP) under section 140. While the Commissioner may not take enforcement action against the CSP directly, any investigation may still involve the CSP.

The parties to an outsourcing arrangement should consider any other contractual obligations governing the handling of personal information and how the CSP may be held accountable for non-compliance under the contract. For example, clauses relating to confidentiality and cyber security or general privacy terms that do not specifically require compliance with the PRIS Act.

Example 3 – A PRIS compliance clause is *not* included in the State services contract

A WA local government (the Council) enters a contract with a Market Research Company (Company) to conduct a survey of residents at a public event. The contract does not include a PRIS compliance clause.

As the contract does not include a PRIS compliance clause, the Council will remain accountable for the Company's handling of personal information. If the actions of the Company in undertaking the survey interferes with the privacy of individuals, enforcement action under the PRIS Act may be taken against the Council only. However, the Commissioner's investigation may also consider the actions of the Company which may impact its findings against the Council.

How PRIS is dealt with in standard Western Australian government contracts

The inclusion of a PRIS compliance clause may not be appropriate in all circumstances. Depending on the nature of the services and the capability of the service provider, an outsourcing entity may wish to retain accountability for compliance with the PRIS Act under the outsourcing arrangement.

The Department of Treasury and Finance (**DTF**) has amended its suite of contracts to include clauses that address PRIS where appropriate. An example of how a standard WA government contract may deal with PRIS requirements is set out below.

Outsourcing entities seeking to amend or use other forms of contracts such as works contracts, or bespoke goods and services contracts, should contact DTF or seek legal advice as to the appropriate clause to include in those contracts.

Example 4 – The General Conditions contain a choice of PRIS accountability clauses

The DTF's *General Conditions of Contract* (the **General Conditions**) for goods and services contracts is an example of a WA government contract where the outsourcing entity can determine whether or not a PRIS compliance clause is appropriate. For outsourcing entities seeking advice regarding these clauses, refer to the guidance text provided by the DTF in the General Conditions.

Clause 25 (*Privacy*) of the General Conditions allows the outsourcing entity to choose from:

1. **No PRIS compliance clause - General Conditions clause 25.1 -** requires the CSP to assist the outsourcing entity to comply with its PRIS Act obligations and requires the CSP to comply with the Australian Privacy Principles set out in the *Privacy Act 1988* (Cth) (irrespective of whether the CSP is an organisation bound by that Act). Under this option, the outsourcing entity remains accountable under the PRIS Act for the CSP's handling of personal information under the contract.
2. **PRIS compliance clause - General Conditions clause 25.2 -** requires the outsourcing entity to select the special condition in Schedule 1 of the Request to activate the PRIS compliance clause in the General Conditions. This clause requires the CSP to comply with the substantive privacy obligations contained in the PRIS Act, including the IPPs, in relation to the handling of personal information under the contract. Under this option, regulatory enforcement action under the PRIS Act may be taken directly against the CSP.

To determine which clause should be used, the outsourcing entity needs to consider a range of factors, including those listed in the drafting instruction in the privacy special condition in Schedule 1 of DTF's Request templates and in this guidance. Relevant factors may include the nature of the contract, the amount and sensitivity of any personal information handled, the privacy maturity of the CSP and other privacy risks associated with the contract. For more information about the factors to consider see 'Managing supply chain risks' below.

Managing supply chain privacy risks

What does an outsourcing entity need to consider when entering a services contract?

It is the responsibility of the outsourcing entity to manage the privacy risks associated with engaging a third party – from pre-procurement planning, due diligence, contracting, service delivery through to the conclusion of the services.

The contractual decisions an outsourcing entity makes in relation to privacy is only one aspect of how an outsourcing entity manages privacy risk. Importantly, the inclusion of a PRIS compliance clause does not absolve an outsourcing entity of these responsibilities.

Procurement planning

At the beginning of the procurement process, an outsourcing entity should consider the privacy risks associated with engaging a third-party service provider and the strategies to manage and mitigate those risks.

Will the CSP require access to personal information?

The most effective way to minimise the privacy risk associated with engaging a CSP is to limit the amount and sensitivity of personal information to which the CSP has access.

The first question an outsourcing entity should ask is whether the services can be performed without providing personal information. Where the CSP does require access to personal information, consideration should be given to how to limit the amount and sensitivity of personal information to which the CSP has access. For example, can the services be performed with aggregated, pseudonymised or even de-identified information?

General due diligence

The outsourcing entity should undertake appropriate due diligence to satisfy itself the preferred CSP can uphold the privacy of any personal information it handles in connection with a State services contract. This might include asking for information and evidence of the following matters in the tender documentation:

- Existing privacy obligations (for example, whether the CSP currently complies with the *Privacy Act 1988* (Cth)).
- Existing policies and procedures related to the handling of personal information (including evidence demonstrating they are consistently applied).
- The CSP's existing cyber security practices and any associated certifications.
- The CSP's use of third parties and whether they will be involved in the processing of personal information under the contract.
- Whether the CSP has been involved in any prior data breaches.
- Examples of where the CSP has successfully provided services in the past to other customers handling personal information in similar volumes with similar sensitivity.

Information from the CSP as part of the due diligence process can help inform how personal information is managed under the contract. Where the outsourcing entity identifies the CSP cannot meet the PRIS Act obligations, it should consider whether to proceed with the contract and, if it does proceed, how to support the CSP to uplift its privacy practices.

Assessing the privacy risks

Where the function or activity to be performed under the contract is a high privacy impact function or activity, the outsourcing entity is required under section 79 of the PRIS Act to undertake a privacy impact assessment (PIA). Even if a PIA is not required, a PIA is a useful tool to assist the outsourcing entity in assessing the privacy risks associated with the outsourcing arrangement.

What does a CSP need to consider when entering a State services contract?

What privacy laws apply?

A CSP should be clear at the outset what privacy laws and regulatory framework apply to its handling of personal information under the contract. To understand when the PRIS Act applies to a CSP's handling of personal information see the section titled 'The PRIS Act and State services contracts'.

Many larger CSPs may already have obligations under the *Privacy Act 1988* (Cth). However, where a contract includes a PRIS compliance clause, the CSP will be directly bound by the PRIS Act in relation to the personal information it handles under the contract and enforcement action can be taken directly against the CSP. Importantly, section 7B(5) of the *Privacy Act 1988* (Cth) expressly gives way to state regulation where the handling is for the purpose of performing obligations under a State services contract.

Where a CSP handles personal information outside of a State services contract, for example in relation to non-government contracts, the PRIS Act will not apply. However, other laws, such as the *Privacy Act 1988* (Cth) may apply.

Example 5 – A CSP may have to comply with different privacy laws under different contracts

A professional services company (the Company) provides security operations center (SOC) services to a WA government Department (the Department). The Company also provides SOC services to a supermarket chain. In each case, the Company has access to significant amounts of personal information contained in metadata and system logs.

The Company's contract with the Department includes a PRIS compliance clause, and the Company is required to comply with the PRIS Act when performing its obligations under the State services contract.

The Company is not required to comply with the PRIS Act in relation to personal information it handles as part of the contract with the supermarket chain. However, it may be required to comply with any other applicable privacy laws or contractual provisions, including the *Privacy Act 1988* (Cth).

To manage the Company's obligations under these different laws, the Company has established a privacy management system designed to support compliance with its obligations.

As part of its engagement planning procedures with the Department, the CSP considers whether its privacy processes need to be augmented to meet any PRIS obligations under the contract.

What personal information will be handled under the contract?

The PRIS Act imposes obligations on the handling of personal information, and places additional requirements on the handling of sensitive personal information. The PRIS Act also places specific obligations on the handling of de-identified information.

Before entering a State services contract, a CSP should understand the type and volume of personal information it will need to receive or access to deliver the services. This will help the CSP to understand the privacy risks involved and the privacy management strategies it will need to implement.

The following examples illustrate how the privacy risks and appropriate mitigation strategies are likely to be different depending on the nature of the outsourcing arrangement and the personal information involved:

Scenario	Example privacy risk & mitigation*
A CSP collects personal information in the course of providing services directly to members of the public on behalf of the outsourcing entity.	**Risk** – personal information is collected unlawfully, without providing appropriate transparency as required by IPP 1. **Example mitigation** – The CSP works with the outsourcing entity to: (1) identify what information is necessary to deliver the service; (2) ensure the collection is fair and reasonable; (3) provide an appropriate collection notice; and (4) obtain any necessary consents.
A CSP provides external audit services to an outsourcing entity which involves analysing	**Risk** – Unauthorised access of the payroll information in contravention of IPP 4. **Example mitigation** – The CSP implements appropriate security controls. Access is restricted to CSP personnel with a need to know.

samples of payroll information.	Processes are implemented to ensure payroll information in the CSP's possession is destroyed or returned when the contract concludes.
A CSP forecasts the demand for flu vaccinations using a large de-identified dataset of historical vaccination records.	**Risk** – Re-identification of the information in contravention of IPP 11. **Example mitigation** – The CSP implements controls to ensure the dataset cannot be reidentified, including appropriate staff training, and external testing. Access is restricted to personnel with a need to know.

*The table above does not provide a comprehensive list of all possible risks, the examples are for illustrative purposes only.

Aligning expectations for the handling of personal information

In an outsourcing arrangement, both the outsourcing entity and the CSP retain a level of responsibility for the handling of personal information. It is important the parties understand the other party's expectations for how personal information will be handled and any division of responsibilities between them including:

- Which party is responsible for collecting personal information and any collection notices that need to be provided? (IPP 1 and IPP 8)
- Does the CSP have any discretion to determine how personal information is used and disclosed (including disclosures overseas)? (IPP 2 and IPP 9)
- What are the respective responsibilities of the outsourcing entity and the CSP to ensure the quality and security of personal information? (IPP 3 and IPP 4)
- Who is responsible for undertaking any assessments or notifications required under the PRIS Act and where might input be required from the other party? (IPP 10, Privacy Impact Assessments and Notifiable Information Breaches)
- How will the parties manage any requests for access or correction of personal information, or respond to complaints? (IPP 6 and Complaints)
- What is the process for destroying or returning any personal information at the end of the contract (taking into account any record keeping obligations)? (IPP 4 and IPP 11)

The parties should also consider the extent to which any subcontractors are responsible for handling any personal information under the contract.

Monitoring privacy risks during an outsourcing arrangement

Privacy risks may evolve over the course of an outsourcing arrangement, particularly where the arrangement lasts for multiple years. The outsourcing entity should consider what monitoring and assurance processes are required to help ensure personal information continues to be handled responsibly for the duration of the contract.

What level of monitoring is appropriate will vary depending on the nature of the services and the privacy risks involved. Examples of monitoring might include requiring:

- Periodic touch points with the CSP to discuss what privacy mitigations have been implemented and any challenges or changes to the privacy risk profile of the outsourcing arrangement.
- The CSP reports on key privacy metrics.
- Evidence of the currency of any relevant certifications.
- Evidence of current security audit or testing results (such as a SOC 2 Type II or IRAP assessment report or annual penetration test results).

- Contractual obligations to notify the outsourcing entity of events that may impact on the CSP or the outsourcing entity's ability to manage its privacy obligations.
- Periodic recompletion of privacy and security questionnaires (or confirmation that nothing has changed from previous responses).
- Periodic auditing of the CSP's privacy and security controls.

Example 6 – Outsourcing entity due diligence & monitoring

A WA government Department (Department) is planning to procure a new Software-as-a-Service (SaaS) customer relationship management system. The system will be used to store large amounts of personal information including, in some cases, sensitive personal information.

As part of the tender process, the Department should ask vendors responding to the request to provide information and evidence of their current privacy and security practices. This might include, evidence of current security certifications, confirmation they are able to meet the requirements of the current WA Cyber Security Policy and evidence of how privacy has been embedded into the design of the system.

The Department may also consider whether the contract enables them to periodically request information from the successful vendor to provide assurance personal information is being handled in accordance with the contract and the requirements of the PRIS Act.

What does the PRIS Act require CSPs to do?

Where a State services contract includes a PRIS compliance clause, a CSP must comply with the substantive privacy provisions contained in Part 2 of the PRIS Act and the IPPs contained in Schedule 1 when handling personal information under the contract. Part 2 Division 11 of the PRIS Act sets out how the PRIS Act and IPPs apply to CSPs.

Handle personal information in accordance with the IPPs

The PRIS Act contains 11 IPPs setting out the minimum requirements for handling personal information from collection through to destruction. For more information about the IPPs, please see the guidance published on the OIC website, including the full text of the IPPs and the OIC's summary Information Privacy Principles Summary.

Example 7 – IPP 6 Access and correction

Under IPP 6 an individual can request access to, or correction of, their personal information held by a CSP. If the CSP receives a request for access or correction under IPP 6 it must notify and consult with the outsourcing entity about the request. The CSP must make a decision about the request for access or correction as soon as practicable, but no later than 45 days after the request was made. If the CSP refuses to give access or correct the personal information, it must give an individual valid reasons. (See also section 132 of the PRIS Act).

Understanding the differences between the PRIS Act and the *Privacy Act 1988* (Cth)

The IPPs share many common features with the Australian Privacy Principles (APPs) contained in the *Privacy Act 1988* (Cth). However, the PRIS Act goes further than the APPs in a number of important ways:

- **Fair and reasonable** – the IPPs require that the collection, use and disclosure of personal information is fair and reasonable in the circumstances taking into account certain matters (see IPP 1.4 and IPP 2.2). Importantly, the requirement for a collection, use or disclosure to be fair and reasonable applies irrespective of whether an individual has consented to the handling of their personal information.
- **Automated decision making** – IPP 10 requires the following actions to be taken where an automated decision-making process involving personal information is used to make significant decisions about individuals:
    1) Conduct an impact assessment
    2) Be transparent about the use of the automated decision-making process, and
    3) Provide an option for human intervention in the process.

    For more information see the OIC's resource Privacy and accountability in automated-decision making.
- **De-identified information** – IPP 11 and IPP 9 include obligations relating to de-identified information. IPP 11 requires reasonable steps be taken to protect de-identified information from misuse and loss and from unauthorised re-identification, access, modification or disclosure. It also regulates the circumstances in which de-identified information may be re-identified. IPP 9 imposes similar requirements in relation to the transfer of de-identified information outside of Australia.
- **Privacy Impact Assessments (PIA)** – the PRIS Act requires a PIA to be undertaken before performing or making a significant change to the way personal information is handled as part of, a 'high privacy impact function or activity' (sections 79 and 137 of the PRIS Act).

A CSP with an existing privacy management system designed to uphold the APPs will provide a good foundation for compliance with the IPPs.

Privacy complaints

Under the PRIS Act individuals have the right to make a complaint about an alleged interference with their privacy to the Commissioner (section 82 of the PRIS Act). As a general rule, the Commissioner will decline to investigate a complaint where the complainant has not complained to the entity first (section 90 of the PRIS Act).

In most cases, the individual will make their complaint to the entity with which they have an established relationship. Depending on the nature of the outsourcing arrangement, this may not be the entity that engaged in the relevant act or practice that is the subject of the complaint. For example, an individual may complain to the outsourcing entity because they have received a service from that entity when, in fact, it is the actions of the CSP that is the subject of their complaint.

When entering a State services contract, the CSP and outsourcing entity should establish a protocol for handling complaints related to the contract. This will help ensure complaints are escalated and handled appropriately irrespective of which entity receives the complaint in the first instance.

Where the complaint relates to the actions of a CSP and the contract includes a PRIS compliance clause, the Commissioner may investigate the actions of the CSP to determine whether there has been an interference with the privacy of the complainant.

Where the complaint relates to the actions of a CSP and the contract does *not* include a PRIS compliance clause, the Commissioner may investigate the acts or practices as if the outsourcing entity had undertaken them. In the course of the investigation, the Commissioner may exercise its powers to request information or documents to support that investigation from the CSP.

Under the PRIS Act, the Commissioner has enforcement powers, including the power to make a determination that an individual's privacy has been interfered with, order compensation or require certain actions be undertaken (section 104 of the PRIS Act). Importantly, even where the outsourcing entity remains accountable, a determination may still outline the CSP's role in the matter.

Notifiable information breach

From 1 January 2027, the notifiable information breach provisions of the PRIS Act will commence (Part 2 Division 6 of the PRIS Act). If the contract includes a PRIS compliance clause, CSPs must comply with these provisions (section 134 of the PRIS Act).

A CSP's contract with an outsourcing entity may also contain obligations with respect to incidents involving personal information, including an obligation to notify the outsourcing entity about any suspected loss, unauthorised disclosure of, or access to, personal information (a suspected information breach). Therefore, it is important when entering a State services contract, the parties agree how they will cooperate in the event of a suspected information breach, including how they will manage any notification obligations under the PRIS Act.

Office of the
Information Commissioner
Western Australia

Address: Albert Facey House, 469 Wellington St, Perth WA 6000, Australia
Website: www.oic.wa.gov.au • **Telephone:** +61 8 6551 7888
Freecall (WA country): 1800 621 244 • **Email:** info@oic.wa.gov.au

The independent regulator fostering trust and accountability in WA through privacy and freedom of information.