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

Privacy 101 – Trainer's Guide

An introduction to the privacy provisions of the *Privacy and Responsible Information Sharing Act 2024* (WA)

A practical resource for Privacy Officers and PRIS champions.

This resource can be tailored to suit the specific context of the audience. It supports the delivery of consistent, accessible privacy training to people working in the Western Australian public sector.

Office of the Information Commissioner
Western Australia

Publication date: 28/05/26

Version Control: 01

How to use this resource

Who should deliver this training?

This trainer's guide and the accompanying PowerPoint are designed to assist Privacy Officers and PRIS champions (you) in the delivery of training to staff.

Who is the audience?

Staff employed by, or providing services to, an IPP entity who handle personal information or who are interested in learning about their own privacy rights.

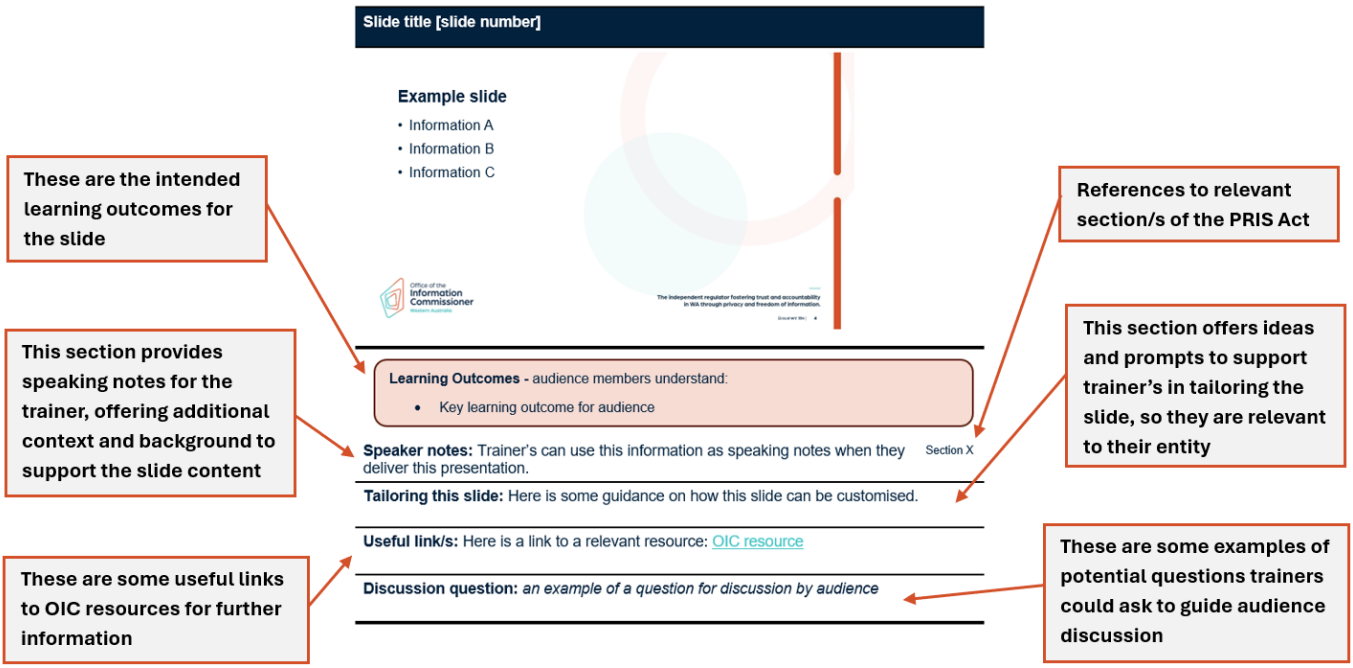
Tailoring the PowerPoint slides for your entity

You are encouraged to customise the PowerPoint slides to ensure they are relevant to the activities and functions of your entity. The slides may be adapted to your entity's brand template, however the OIC must be acknowledged as the original source together with a clear statement the slides have been modified where modification has occurred.

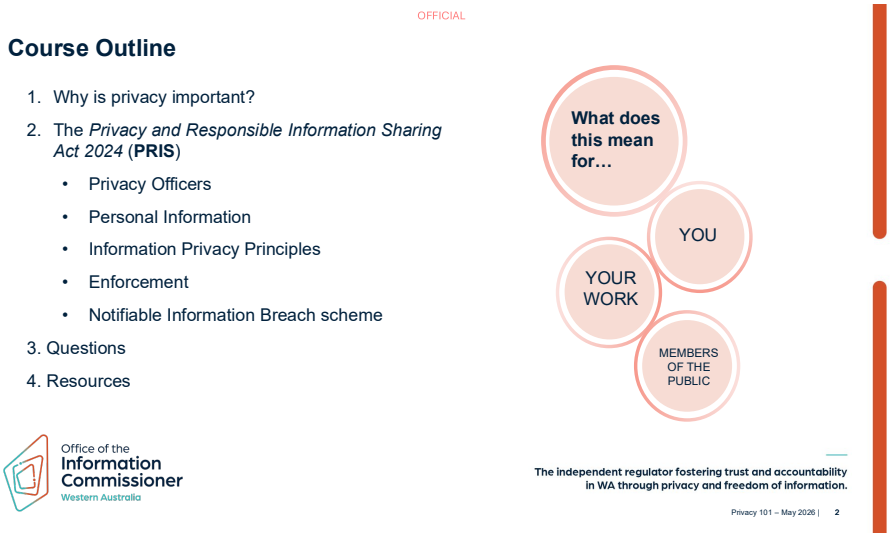
How should this presentation be delivered?

This presentation should be delivered in a way that is appropriate for your audience. It does not need to be delivered as a single session. You may choose to divide the presentation and deliver it over a series of smaller sessions.

Using this trainer's guide:



The *Privacy and Responsible Information Sharing Act 2024* [slide 2]



Learning Outcomes: audience members understand that this presentation is relevant to them because they have responsibilities in relation to personal information.

Speaker notes: This slide provides an overview of today's presentation.

The audience is encouraged to consider how privacy is relevant to each of them and the work they do for the entity. The audience might also be encouraged to consider how it is relevant to each of them as members of the public.

The *Privacy and Responsible Information Sharing Act 2024* **(WA)** (**PRIS Act**) establishes a comprehensive framework governing the collection, use, disclosure and management of personal information and introduces obligations for the handling of de-identified information. It also is the first legislation in Australia to directly regulate the use of automated decision-making where it involves the use of personal information.

The PRIS Act gives effect to the public's expectation of accountability and transparency regarding the handling of their personal information. Everyone in the WA public sector has a role in giving effect to these expectations.

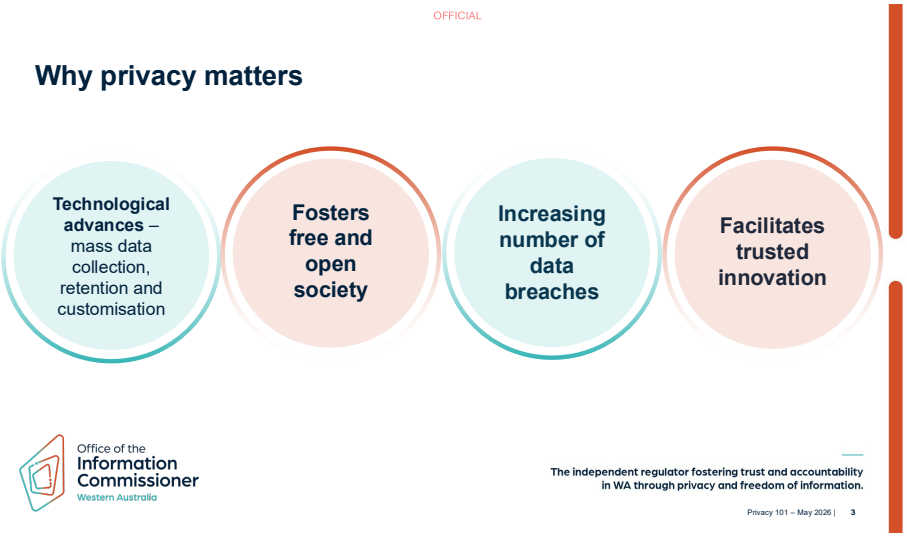
By the end of this presentation, the audience will be equipped to answer the following PRIS related questions as they relate to their work:

- Who is your entity's Privacy Officer and what is their role?
- What is personal information?
- What are the Information Privacy Principles?
- How is the PRIS Act enforced?
- What to do in the event of a suspected information breach?

AND if they can't answer the questions, they will know where to get help on these questions.

Consider how you might connect your audience to the privacy theme of this presentation. This might include a real story, or a fictitious but plausible scenario, to help illustrate what privacy looks like in practice with your entity.

Why privacy matters [slide 3]



Learning Outcomes: audience members understand that good privacy practice is in everyone's' interest.

Speaker notes: Privacy is important because:

Technological advances

- Rapid evolution of digital technologies has enabled the handling of personal information at scale and this creates new challenges for privacy
- Technology (particularly AI) can process massive volumes of data resulting in large scale customisation.
- Data can be easily shared, aggregated and repurposed beyond the original purpose of collection.

Fosters free and open society

- Privacy supports a free and open society by allowing individuals to go about their lives free from surveillance that may impact on their behaviour.
- For example, the use of surveillance and targeting technologies can shape the information to which people are exposed and manipulate them into making choices that they might not otherwise have made.
- Privacy laws also help protect against discrimination, profiling and unfair treatment.

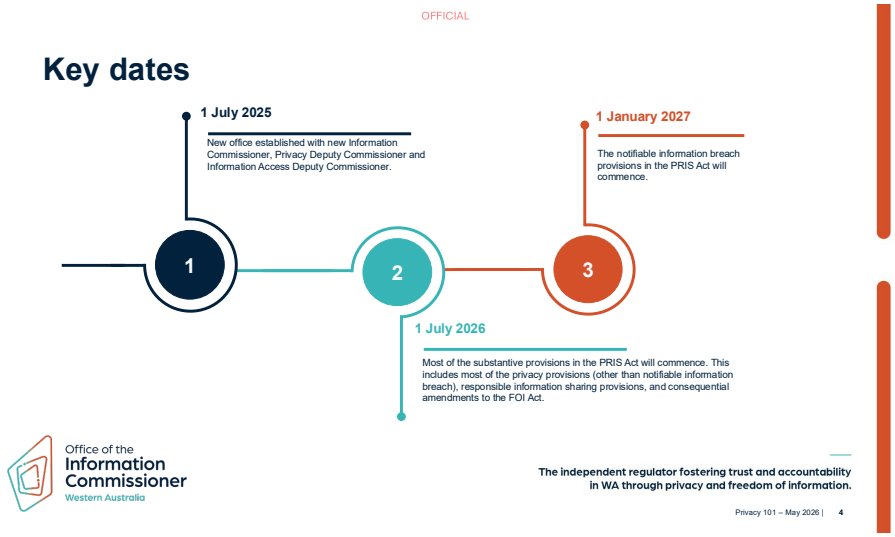
Increasing number of data breaches

- Data breaches are becoming more frequent and sophisticated.
- Breaches can result in a range of privacy harms including identity theft, financial loss, humiliation and emotional injury.
- Strong privacy practices reduce the likelihood and impact of data breaches
- Transparency and accountability after a data breach also helps maintain public confidence.

Facilitates trusted innovation

- Effective privacy laws help members of the public have confidence that using digital technology won't harm them.

Key dates [slide 4]



Learning Outcomes - audience members understand:

- There are two important dates – 1 July 2026, when the substantive privacy provisions of the PRIS Act commence and 1 January 2027, when notifiable breach requirements commence.
- The entity has been preparing for these dates, and good privacy practice should have already commenced

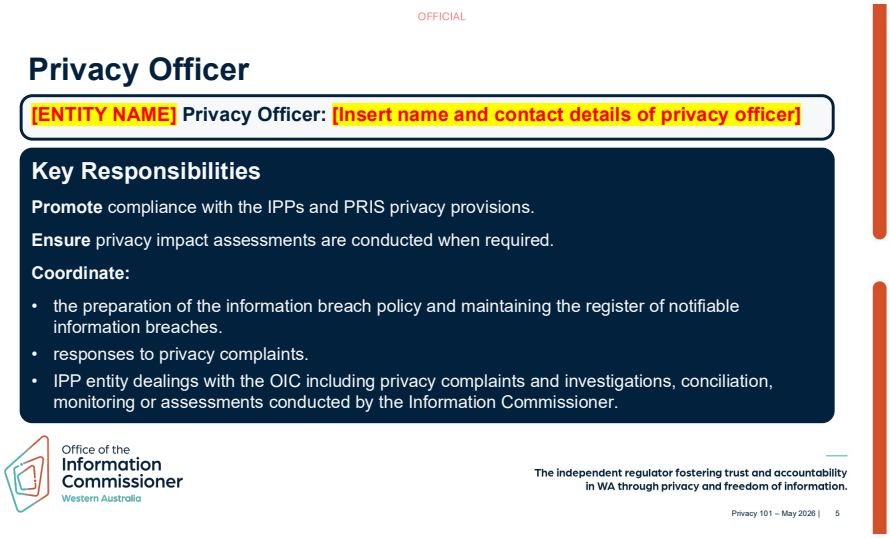
Speaker notes: A new office of the Information Commissioner (the OIC) was established on 1 July 2025, followed by the appointment of the Information Commissioner, Privacy Deputy Commissioner and Information Access Deputy Commissioner.

Most of the privacy provisions come into effect from 1 July 2026.

The notifiable information breach provisions commence 1 January 2027.

Useful link: The OIC has published guidance for IPP entities about how the privacy provisions of the PRIS Act applies to personal information collected before and after 1 July 2026: Personal information collected before and after 1 July 2026

Privacy Officer [slide 5]



Learning Outcomes: audience members will know -

- Who is the entity's Privacy Officer
- What is the role of the Privacy Officer
- How/where they can contact the entity Privacy Officer

Speaker notes: The principal officer of an IPP entity must ensure the appointment of a Privacy Officer.

Section 151

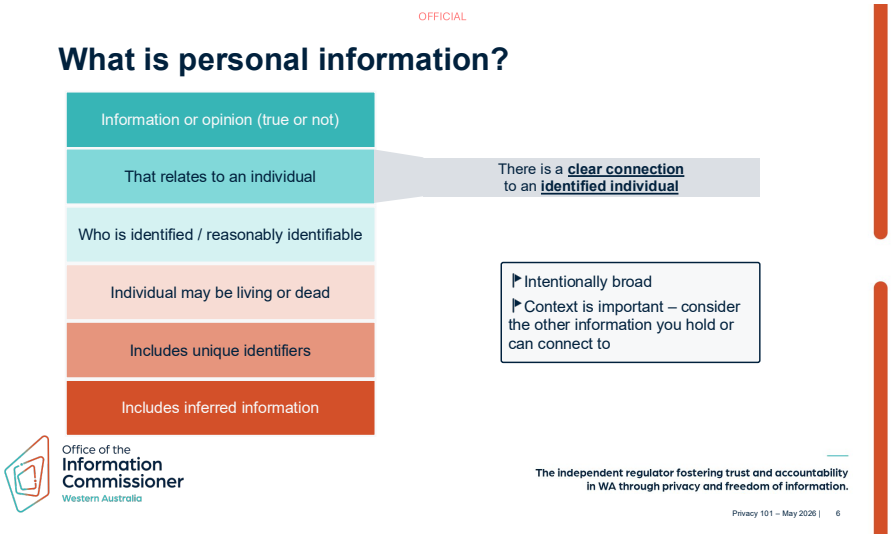
The Privacy Officer must be in a position to influence change in the organisation.

Could be a rotating position across different operational units to leverage diverse expertise and ensure the role sits within an area of agency with privacy priorities.

Tailoring this slide: include the name and contact details of your entity's Privacy Officer. If your entity also has a PRIS Champion or privacy team you may also want to include this information.

Useful link: Who is the Privacy Officer within a public entity?

What is personal information? [slide 6]



Learning Outcomes: audience members have a general understanding of -

- The meaning of personal information, including that it covers a broad range of different kinds of information
- Whether the information they deal with is personal information.

Speaker notes: This PRIS Act is concerned with personal information. It is important to understand what personal information is in order to apply the privacy provisions. Section 4

The definition of personal information is intentionally broad and includes:

- a name, date of birth or address
- a unique identifier, online identifier or pseudonym
- contact information
- information related to an individual's location
- technical or behavioural information in relation to an individual's activities, preferences or identity
- inferred information that relates to an individual, including predictions in relation to an individual's behaviour or preferences and profiles generated from aggregated information
- information that relates to one or more features specific to the physiological, genetic, mental, behavioural, economic, cultural or social identity of an individual

continued

What is personal information? [slide 6] - continued

Speaker notes (continued):

Information or opinion
Personal information can include both objective data and subjective views. Opinions can still be personal information even when they are informal or unverified.

That relates to an individual
For information to be personal information it must 'relate to' an individual. This means there must be a relationship between the individual and the information. There are two parts in determining whether information relates to an individual:

a. there is a clear connection (not distant or vague)
b. the information can be connected to an identified individual (or the identity of the individual is reasonably ascertainable).

Who is identified/ reasonably identifiable
The person does not have to be identified from the information alone. An individual may still be identifiable where the information can be combined with other information (including from other sources) that identifies them. Whether this is possible depends on the context.

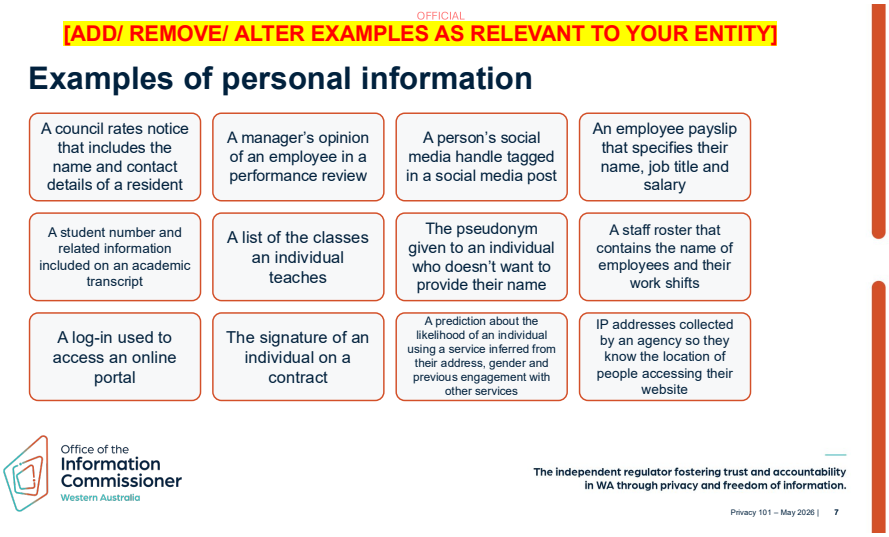
Individual may be living or dead
The definition of personal information includes both living and deceased individuals.

Includes unique identifiers
A unique identifier is a number or other identifier assigned by an entity to an individual to uniquely identify that individual for the purposes of the operations of the entity.

Includes inferred information
Inferred information is information that isn't collected directly from the individual. It is derived or generated from other information.

Note - On and from 1 July 2026, the definition of personal information in the FOI Act will be amended to be the same as the definition of personal information in the PRIS Act.

Examples of personal information [slide 7]



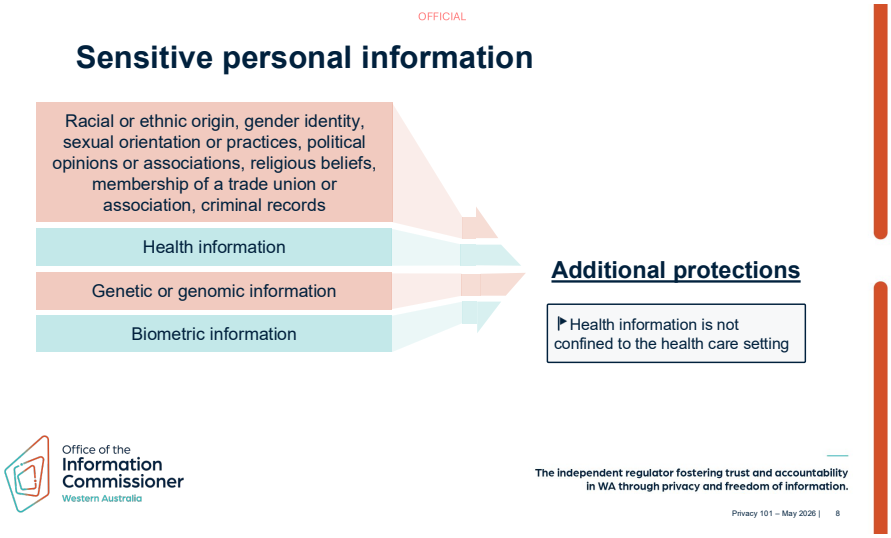
Learning Outcomes: audience members connect with an example or examples that highlight the kind/s of personal information that they may handle as part of their role.

Tailoring this slide: When considering examples relevant to your entity:

- Look beyond the core delivery areas of your entity.
- Consider does your entity collect or generate information about people (including staff), even incidentally.
- Some areas you might consider:
  - HR (recruitment, performance, leave records)
  - Finance (invoices, reimbursements, payroll)
  - IT systems (user accounts, access records)
  - Communications (complaints, social media interactions)
  - Procurement and contract
  - Security (CCTV, access cards)
- Does your entity assign numbers, codes or profiles (unique identifiers) that could identify or single a person out?
- Does your entity create information that could be considered personal?
  - Risk scores based on behaviour or history
  - Analytics that predict future behaviour
- Consider how personal information moves through your entity. Is personal information shared between teams or systems?

Discussion questions: *What types of personal information do you handle as part of your work? Is there information you handle that you're unsure is personal information?*

Sensitive personal information [slide 8]



Learning Outcomes: audience members understand that -

- Sensitive personal information is a subset of personal information and attracts additional protections
- Even if you work outside a health service, the entity is likely to handle health information (which is sensitive information)

Speaker notes: Sensitive personal information is a type of personal information. It includes information that relates to an individual's: Section 4

- racial or ethnic origin; or
- gender identity; or
- sexual orientation or practices; or
- political opinions or associations; or
- religious beliefs; or
- trade union membership or association; or
- criminal record.

Health information

Can relate to:

- the health or disability of an individual at any time.
- an individual's expressed wishes about health services they want or don't want provided to them in the future.
- a health service provided, or to be provided to an individual.

It includes any personal information collected to provide, or in providing a health service.

continued

Sensitive personal information [slide 8]- continued

Speaker notes (continued):

Genetic or genomic information

Genetic information is not defined in the PRIS Act. It can be broadly understood to include information about an individual's genetic makeup.

Biometric Information

Biometric information is not defined in the PRIS Act. It is generally understood to include physical or behavioural characteristics of an individual, often used for identification verification.

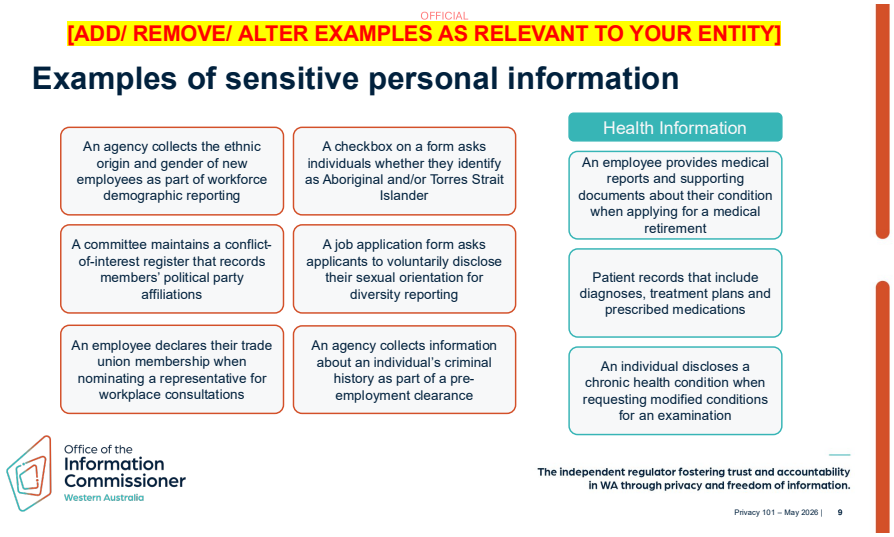
Inferred information

Sensitive personal information derived or generated from other information.

There are additional protections for sensitive personal information.

These additional protections are because sensitive information carries inherent risks to individuals' privacy (and other rights). One of the privacy risks associated with sensitive personal information is discrimination.

Examples of sensitive personal information [slide 9]



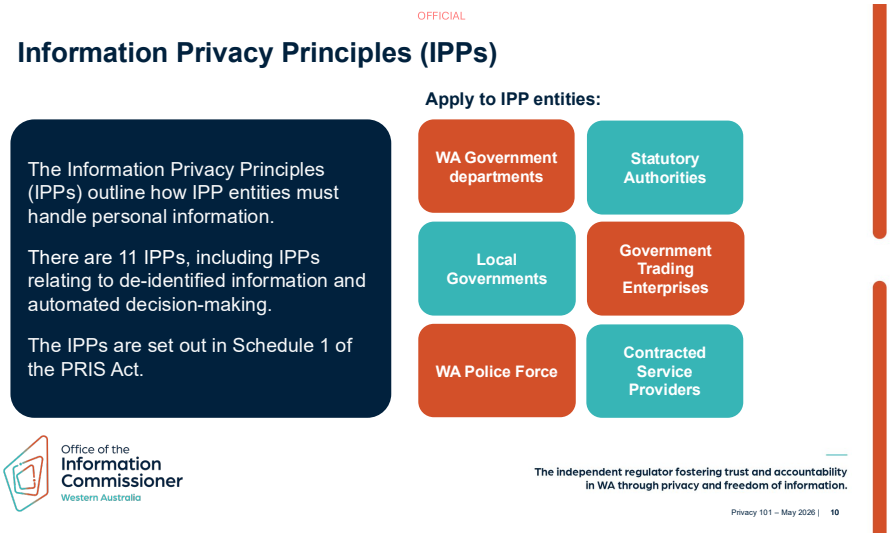
Learning Outcomes: audience members connect with an example that highlights the kind/s of sensitive personal information that they may handle in their role.

Tailoring this slide: When identifying examples of sensitive information relevant to your entity consider:

- Data collected for administrative or compliance purposes
- Health information processed outside of a healthcare setting, such as:
  - Medical certificates
  - Fitness for work or return to work assessments
  - Workers compensation claims
  - Incident reports
  - Applications for retirements on medical grounds
- Information relating to vulnerability or risk, including:
  - Records that identify that someone is at risk of harm
  - Family violence or safeguarding concerns
  - Financial hardship indicators
  - Child protection
  - Use of financial aid or welfare

Discussion question: *What types of sensitive personal information, including health information do you collect or handle as part of your work?*

Information Privacy Principles (IPPs) [slide 10]



Learning Outcomes: audience members understand -

- That the IPPs govern how IPP entities handle personal information
- What an IPP entity is

Speaker notes: The Information Privacy Principles (IPPs) are set out in **schedule 1** of the PRIS Act.

The Information Privacy Principles (IPPs) outline how IPP entities must handle personal information. One way that the PRIS Act and the IPPs go beyond the requirements of other Australian privacy laws, is through the inclusion of specific principles dealing with de-identified information and automated decision-making.

The IPPs apply to IPP entities — Section 20

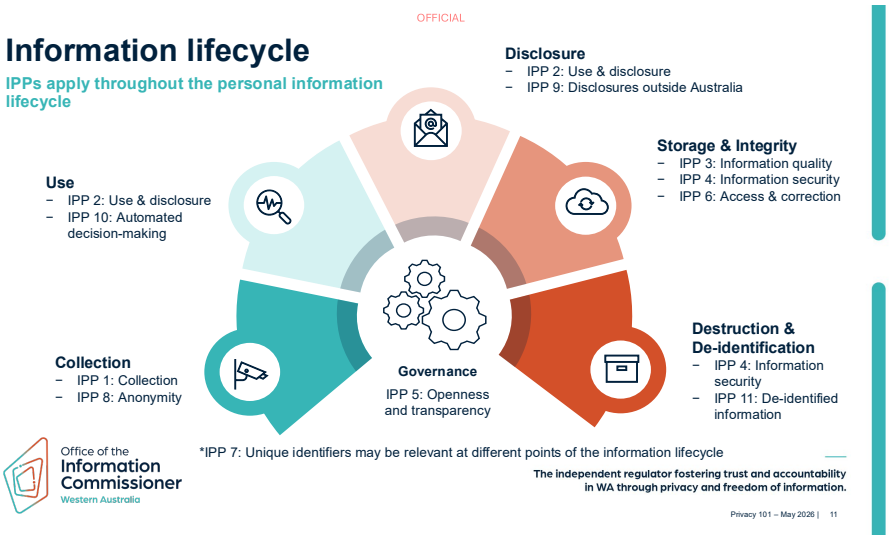
An IPP entity is: — Section 14

- A Minister; or
- A Parliamentary Secretary; or
- A public entity; or
- A contracted service provider.

A public entity includes Western Australian government departments, the WA Police Force, statutory authorities, local governments and government trading enterprises — Section 6

A contracted service provider provides services to or on behalf of a public entity. — Section 8(2)

Information lifecycle [slide 11]

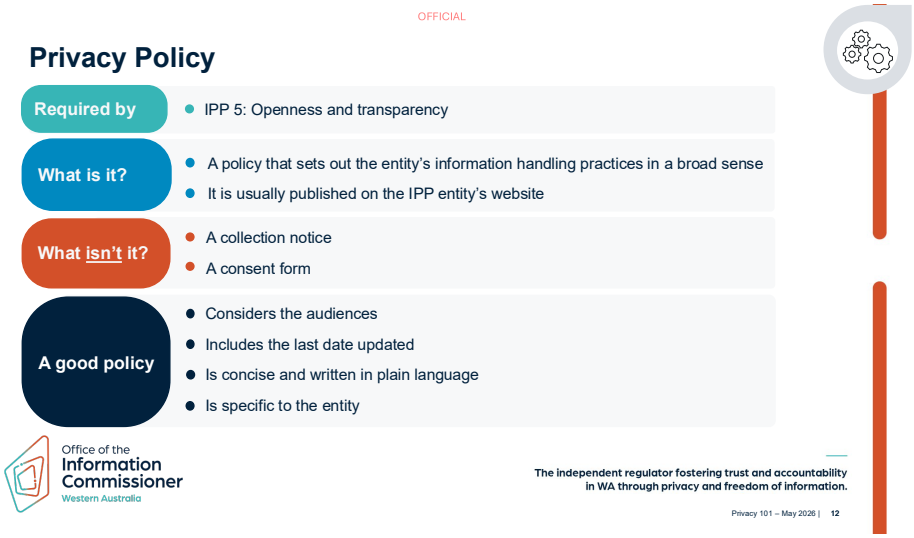


Learning Outcomes: audience members are introduced to fact that privacy requirements apply across the lifecycle of both digital and non-digital information.

Speaker notes:
The IPPs apply to personal information throughout the information lifecycle from collection through to when it is destroyed or de-identified.

This presentation will cover the IPPs with respect to where they sit in this lifecycle.

Privacy Policy [slide 12]



Learning Outcomes: audience members -

- Understand that the entity is required to have a privacy policy.
- Know where to find the entity's privacy policy.

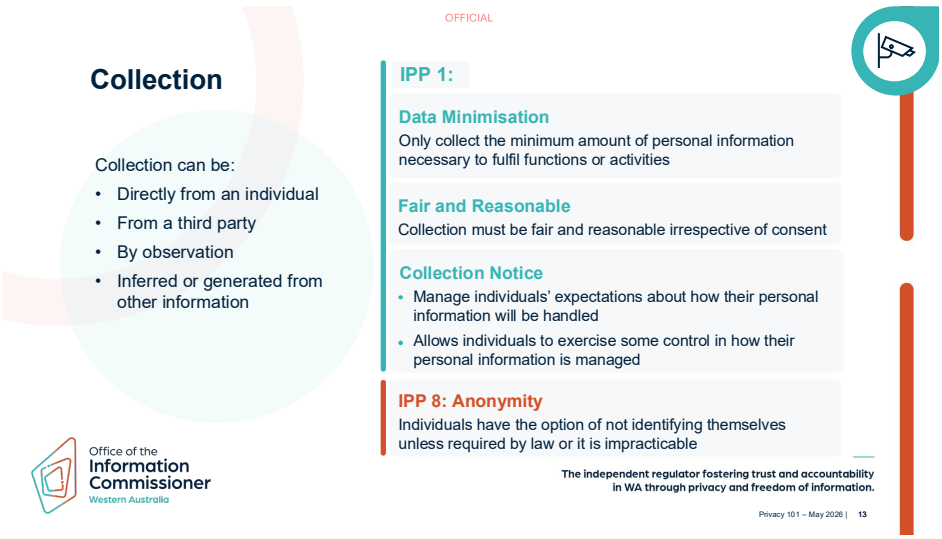
Speaker notes: IPP 5 requires an IPP entity to have a publicly available privacy policy that sets out what personal information it collects and holds, and how and why it handles personal information. The privacy policy must also include whether any personal information is used in automated decision-making.

A privacy policy is different from a collection notice. A privacy policy covers the full range of personal information handling practices across the entity's activities. In contrast, a collection notice is required each time personal information is collected and contains information specific to the particular collection.

A policy that is up-to-date, clear, concise and expressed in plain language supports public confidence in your entity's handling of personal information.

Tailoring this slide: Provide a link to your entity's privacy policy and outline the key features.

Collection [slide 13]



Learning Outcomes: audience members understand that -

- The entity should minimise the personal information it collects ("data minimisation").
- Minimising the amount of personal information collected can help an entity reduce its risk exposure.
- A collection of personal information must be "fair and reasonable"
- When an entity collects personal information, it must provide notice of certain matters (called a 'collection notice').

Speaker notes: The principles for collection are set out in IPP 1: Collection — IPP 1

Collection is the process of obtaining personal information from any source or by any means. Collection includes the collection of personal information directly from an individual, a third party or the creation of new personal information by using or interpreting other information.

Data minimisation

Central to IPP 1 is the principle of 'data minimisation' – collecting only the minimum personal information necessary for a specific purpose.

TIP: Before collecting the information ask 'can I perform this function or activity without personal information or with less personal information?'.

IPP 8: Anonymity

IPP 8: Anonymity gives individuals the option of not identifying themselves when dealing with an IPP entity (except when required by law or impracticable for the IPP entity). — IPP 8

Fair and reasonable

A collection of personal information must also be 'fair and reasonable'. In general, this means the collection should be necessary, not excessive and appropriately balances any impact on privacy. — IPP 1.4

continued

Collection [slide 13] continued

Speaker notes (continued):

Collection Notice

IPP 1.9

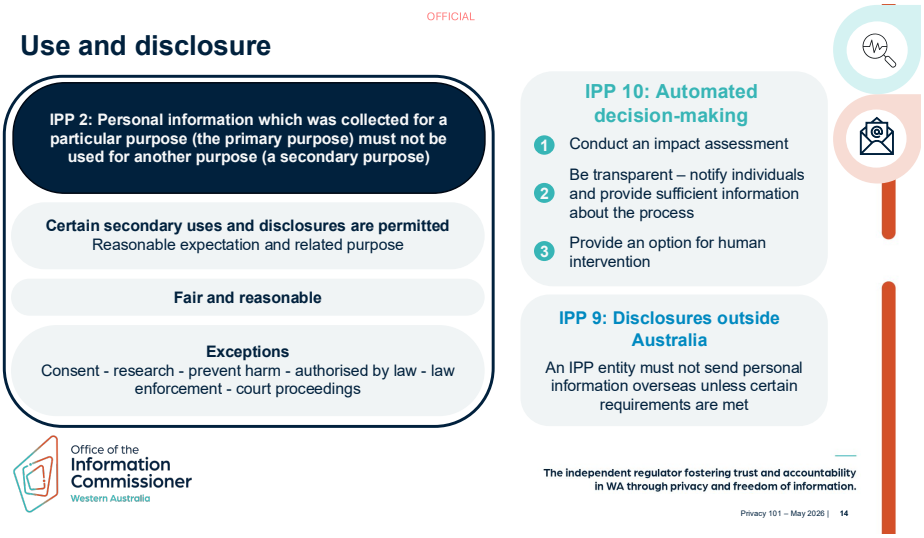
A collection notice:

- Informs individuals about how and why their personal information is being collected, how it will be used and disclosed, and their rights in relation to that personal information.
- Providing this information assist IPP entities to manage individual's expectations around how their personal information is going to be handled.
- A collection notice provides individuals with the necessary information for them to exercise a greater degree of control over the management of their personal information.
- Must be up-to-date, clear, concise and expressed in plain language.
- Generic notices (such as a link to an entity's privacy policy) not specific to the situation do not meet the requirements.
- Using a collection notice as a vehicle for consent is discouraged. If consent is required, it should be sought separately and it should be clear to what the individual is being asked to consent.

Discussion questions: *Is it necessary to collect all of the personal information that you collect in your role? What can you do if you are concerned that you are collecting unnecessary personal information?*

Useful link: What is a collection notice and what should it contain?

Use and disclosure [slide 14]



Learning Outcomes: audience members understand that -

- Personal information should only be used or disclosed for the purpose for which it was collected.
- The collection notice sets the purposes for which personal information is collected.
- Personal information may be used or disclosed for a secondary purpose in certain limited circumstances, including where the individual would reasonably expect the entity to use or disclose the information for the secondary purpose and it is related to the primary purpose.

Speaker notes:

Disclosure is sharing personal information outside the IPP entity, including making the information publicly available.

See section 10 for definition of disclosure

Disclosure does not include the IPP entity disclosing the information to itself or to an officer of the IPP entity, which is regarded as a 'use' of personal information.

Use and disclosure are generally referred to together in the IPPs. Together they can be understood as being about how personal information is used and shared.

A central principle to IPP 2 is purpose limitation – meaning an IPP entity can only use and disclose personal information for the purpose the entity collected it unless an exception applies.

IPP 2.1

IPP 2.1(a)-(b)

<u>Secondary use</u>

Any purpose that is not the purpose for which the personal information was collected is known as a secondary purpose. You can use information for a secondary purpose if:

- The individual would reasonably expect your IPP entity to use or disclose it for that secondary purpose; and
- The secondary use or disclosure is related to the primary purpose.

However, even where this exception applies, the use or disclosure must still be fair and reasonable.

continued

Use and disclosure [slide 14] continued

Speaker notes (continued):

Exceptions

There are a number of exceptions to the purpose limitation principle, including where the use or disclosure is required or authorised by law and where the individual consents to the use or disclosure.

IPP 2.2

Fair and Reasonable

A use or disclosure of personal information must be fair and reasonable in the circumstances. This is called the 'fair and reasonableness test' and it applies irrespective of whether the individual has consented to the use or disclosure.

IPP 2.1(c)-(g)

The fair and reasonableness test is a balancing exercise. IPP 2.2 sets out the matters that must be taken into account, including the necessity of the use or disclosure, the volume and sensitivity of the information, what the individual would reasonably expect and the risk of harm to the individual.

Automated Decision-Making

IPP 10

The PRIS Act is the first legislation in Australia to introduce requirements to directly manage the privacy risks of automated decision making.

See section 16 for definition of:

If an IPP entity uses an automated decision-making process involving personal information to make a significant decision about an individual, they must:

- first conduct an impact assessment
- be transparent by notifying the individual ADM has been used and provide sufficient information about the ADM processes; and

automated decision-making processes

and

significant decision

provide a process by which that individual can request human intervention in relation to that decision.

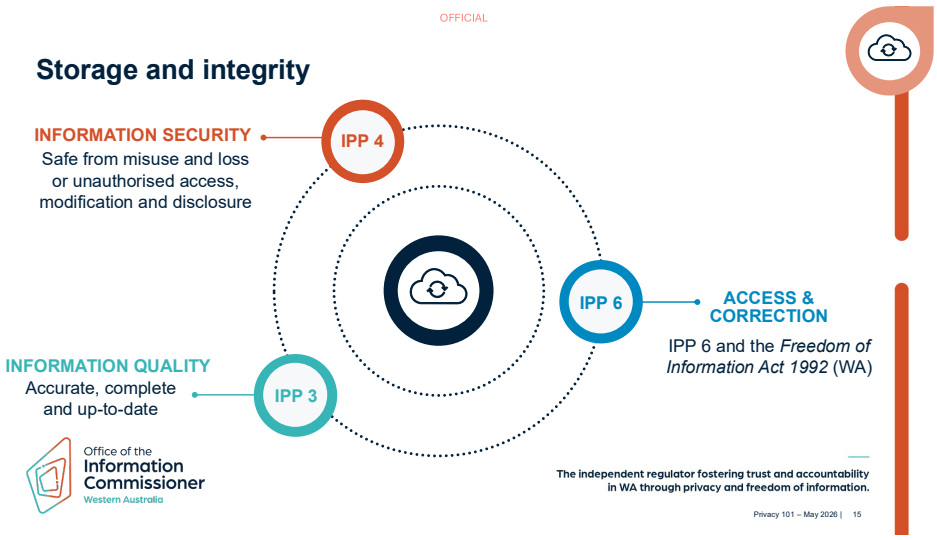
Disclosures outside Australia

IPP 9

An IPP entity must not send personal information overseas unless certain requirements are met. This includes, for example, where the IPP entity has taken reasonable steps to ensure the recipient will handle the information consistently with the IPPs.

Further, an IPP entity must not send de-identified information overseas unless the recipient has appropriate security in place to protect the information and does not try to re-identify it.

Storage and integrity [slide 15]



Learning Outcomes: audience members understand that -

- IPP 3 is critical because decisions are made based on the information the entity holds
- Information security is not just IT's job – everyone plays a part in ensuring the security of digital and non-digital information

Speaker notes: Once personal information has been collected, it must be stored and managed in a way that protects its integrity and safeguards the information from misuse and loss and from unauthorised access, use and disclosure.

IPP 3: Information quality

Information integrity or quality is critical to support sound decision making. This is because an entity can't rely on information that is inaccurate, incomplete or out of date. Poor quality data can lead to incorrect or unlawful decisions, perpetuate misinformation or errors over time and ultimately undermine trust and accountability.

IPP 4: Information security

Without appropriate security safeguards, personal information can be exposed or misused leading to harm to individuals. The protection of personal information is not only the responsibility of your information technology team. There are important steps you can take to maintain the security of personal information, for example: ensuring you limit access to people with a need to know, avoiding sharing sensitive personal information over email and being vigilant to phishing attacks.

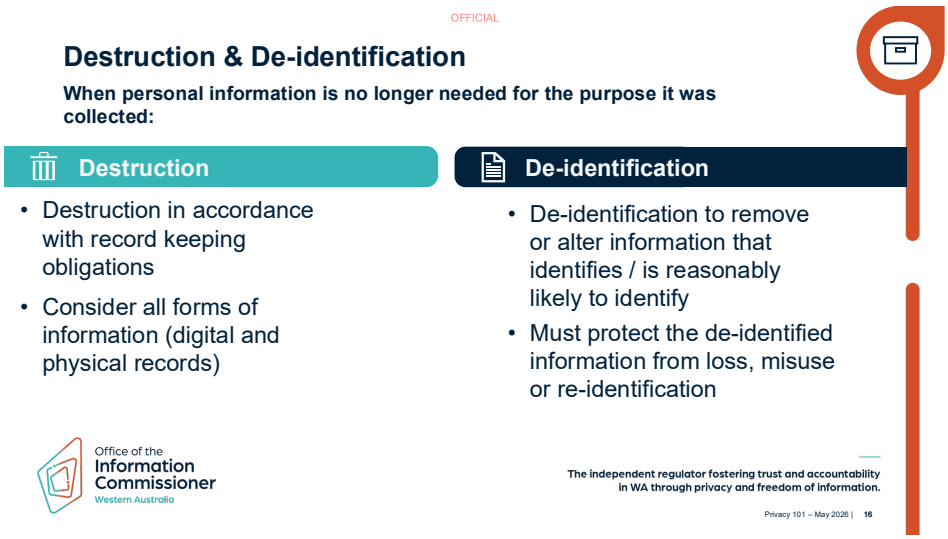
IPP 6: Access and correction

IPP 6 provides individuals with the right to seek access to, or correction of, their personal information where it is held by a contracted service provider.

There is an existing right to access or correct personal information contained in government documents under the *Freedom of Information Act 1992* (WA) and this will continue to operate alongside IPP 6.

No wrong door approach – if the application is made under IPP 6 and it should have been made under FOI then the IPP entity must deal with the application as if it was made under FOI.

Destruction & De-identification [slide 16]



Learning Outcomes: audience members understand that -

- It is good privacy practice and good record keeping practice to only keep what is necessary and are encouraged to familiarise themselves with their entity's record keeping plan.
- Good processes for record destruction minimise risk for entities and the public.

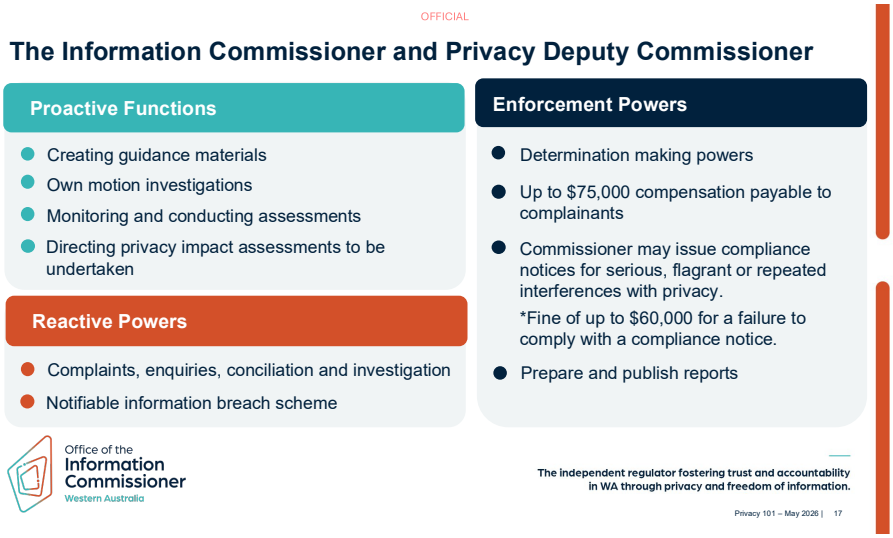
Speaker notes: The final stage of the information lifecycle is what happens when the personal information is no longer needed for the purpose for which it was collected. At this point, IPP entities must either securely destroy or de-identify the information. IPP 4.2

Nothing in the PRIS Act or IPPs limits the operation of the *State Records Act 2000*. Timeframes for retaining information are unchanged and remain per the required retention and disposal authority. Section 153(1)

De-identification of personal information means to modify or apply a process to the information with the result being the identity of the person is not apparent, or the identity of the person cannot be reasonable ascertained from the information. Section 11(1)

However, even when information has been de-identified the IPPs still require the information continues to be protected from misuse and loss and unauthorised access modification or disclosure, as well as from the risk of re-identification. IPP 11

The Information Commissioner and Privacy Deputy Commissioner [slide 17]



Learning Outcomes: audience members are aware that -

- The Information Commissioner and the Privacy Deputy Commissioner have enforcement powers under the PRIS Act.
- The OIC WA provides guidance and deals with enquiries from IPP entities and the public.

Speaker notes: The *Information Commissioner Act 2024* establishes the offices of Information Commissioner and Privacy Deputy Commissioner.

The Office of the Information Commissioner (OIC) has a dual remit covering both privacy and Freedom of Information.

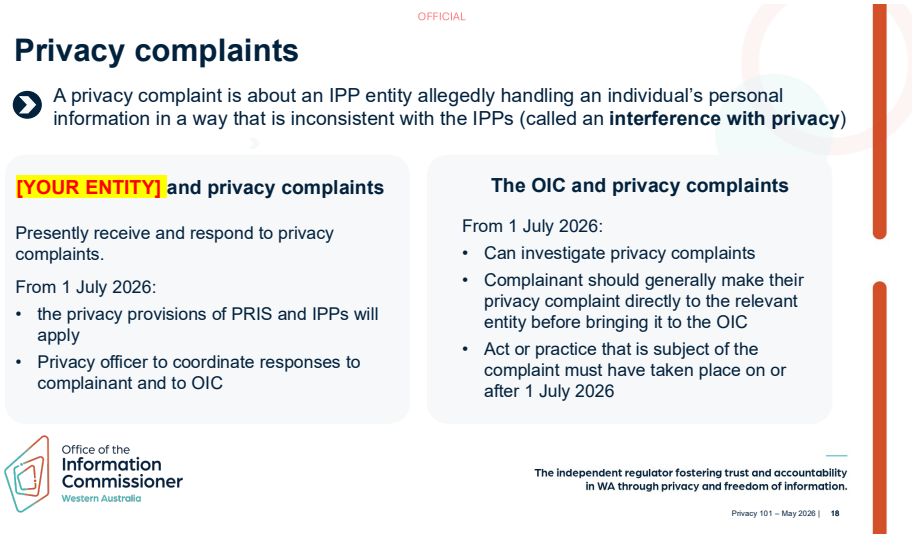
From 1 July 2025 the functions and powers of the Information Commissioner and the Privacy Deputy Commissioner under the PRIS Act include:

- Ensuring the WA public sector and members of the public are aware of their privacy obligations and rights under the PRIS Act including the IPPs.
- Promoting the objects of the PRIS Act and compliance with the privacy obligations in the PRIS Act and the IPPs.
- Developing information and materials in relation to upholding privacy.

From 1 July 2026 the functions and powers of the Information Commissioner and the Privacy Deputy Commissioner will also include:

- Dealing with privacy complaints
- Investigating and enforcing compliance with the privacy obligations in the PRIS Act
- Approving or amending Privacy Codes of Practice
- Dealing with Public Interest Determination applications
- Undertaking reviews, preparing reports and making recommendations on matters relating to privacy.

Privacy complaints [slide 18]



Learning Outcomes: audience members understand that -

- From 1 July 2026, individuals can make a complaint to the Information Commissioner that the entity has handled their personal information in a way that is inconsistent with the IPPs.
- Privacy complaints must generally be made to the relevant IPP entity before the OIC will deal with a complaint.
- Whether the entity has a complaint handling process already in place.

Speaker notes: A privacy complaint is about an IPP entity handling an individual's personal information in a way that is inconsistent with the IPPs or the notifiable information breach provisions contained in the PRIS Act (referred to as "an alleged interference with the privacy of an individual").

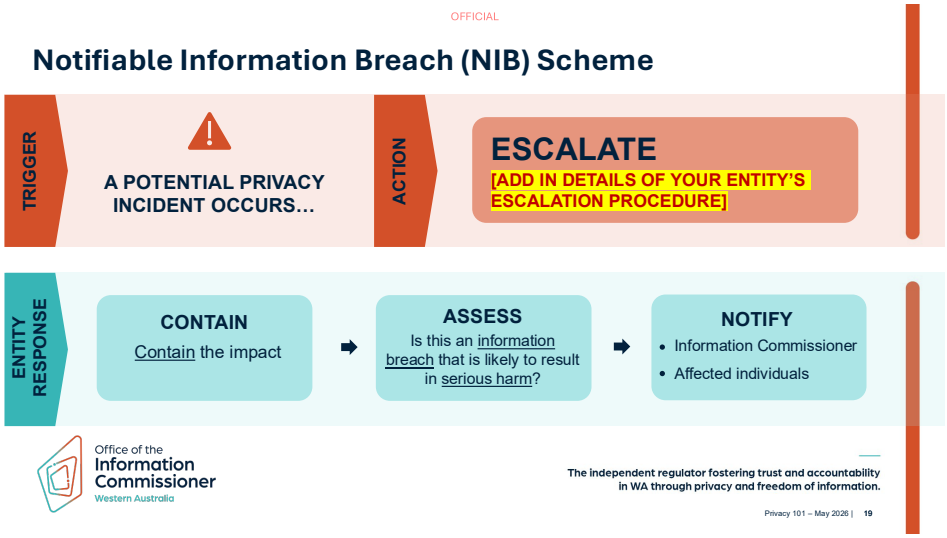
The Privacy Officer is responsible for coordinating the IPP entity's response to privacy complaints, this may mean working with an existing complaints officer/team where one exists. They also coordinate the IPP entity's dealings with the OIC in relation to privacy complaints. Section 151

<u>The OIC and privacy complaints</u>
From 1 July 2026, the OIC will have jurisdiction to investigate and resolve privacy complaints. As a general rule, the relevant act or practice the subject of the complaint must have taken place on or after 1 July 2026. Section 82

The OIC can decline a complaint if the complainant has not first complained directly to the relevant IPP entity. The IPP entity must have been given a reasonable time to respond to the complaint. Section 90

Tailoring this slide: Insert the name of your IPP entity in the highlighted area. Provide an overview and a link to your entity's complaints handling process.

Notifiable Information Breach Scheme [slide 19]



Learning Outcomes: audience members are aware -

- Of the definition of a notifiable information breach.
- Where to locate the entity's information breach policy.
- Who they should escalate to in the event they identify a potential privacy incident

Speaker notes: The Notifiable Information Breach (NIB) scheme will come into effect on 1 January 2027. Under this scheme, IPP entities must notify affected individuals, and the Information Commissioner, if there is unauthorised access to, or unauthorised disclosure of, or loss of personal information held by the entity and the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.

The key message for all staff is that if a potential privacy incident occurs, they must escalate it for response.

Entity Response

Contain the impact – take immediate steps to stop or limit the incident

An assessment should be performed in response to the privacy incident to determine whether it has resulted in a notifiable information breach. This includes an assessment of the liklihood of serious harm occuring. — Section 57, Section 59

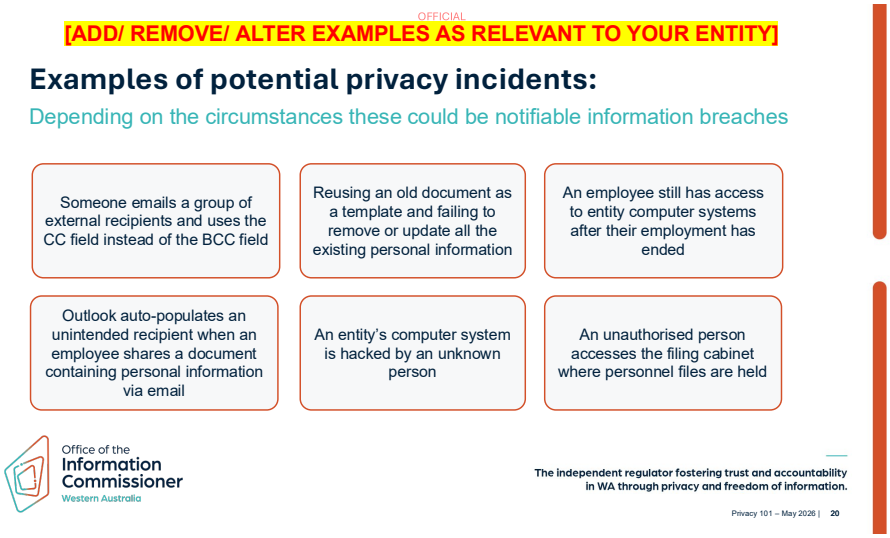
Where a privacy incident is assessed as a notifiable information breach, your entity must:

- give the Information Commissioner written notice, and
- take all reasonable steps to give written notice to all affected individuals

— Section 62, Section 63

Tailoring this slide: Add in the details of your entity's information breach procedure outlining how audience members should escalate suspected information breaches. Provide a link to your entity's information breach policy.

Examples of information breaches [slide 20]

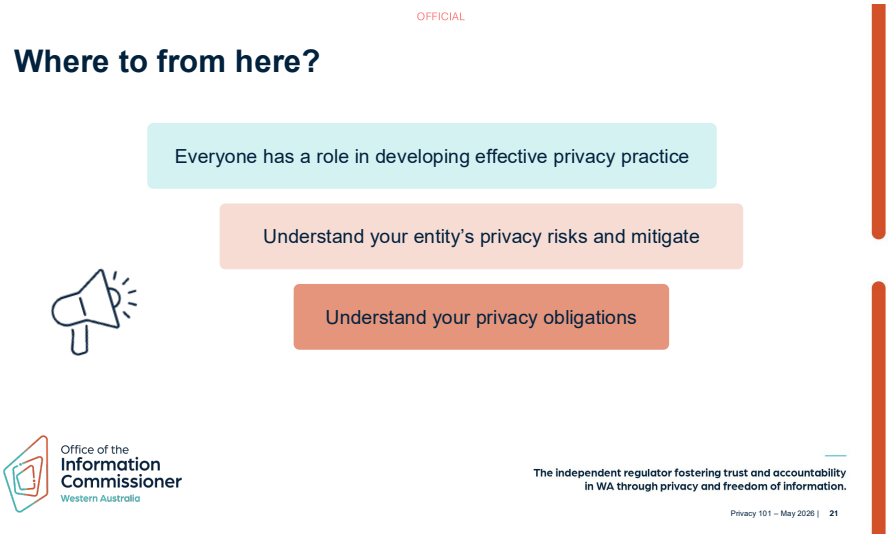


Learning Outcomes: audience members will connect with an example or examples that highlight the way that an information breach occurs.

Tailoring this slide: When providing examples relevant to your entity:

- Consider human errors, what mistakes could realistically happen?
- Consider systems and technology risks:
  - Integration issues between systems
  - Access controls or permissions
  - Cyber security incidents
- Consider the risks posed by the physical environment:
  - Can sensitive conversations be easily overheard?
  - Are records containing personal information behind a locked door?
  - The location of printers, computers or other shared resources
- Think about past incidents or near misses

Where to from here? [slide 21]



Learning Outcomes: audience members -

- Understand that they each have a role to play in upholding privacy
- Know where they can go for more information
- Are aware of your entity's privacy priorities
- Are empowered to identify ways to embed good privacy practices into their business areas.

Speaker notes:

Everyone working in public entities has a role to play in building effective privacy practice. This starts by understanding your privacy obligations. For your audience this starts with, knowing:

- Who their entity's Privacy Officer is;
- About the IPPs and how they can be applied in their day-to-day role within their entity;
- Where they can find their entity's privacy policy;
- That privacy complaints are handled by their entity and who to contact in the event they receive a complaint;
- That the notifiable information breach scheme will come into effect in January 2027 and they should follow their entity's information breach policy when they suspect there had been a breach.

Tailoring this slide: Use the information in the presentation to provide your audience with a "call to action":

- Align the call to action with your entity's privacy priorities.
- Provide specific, actionable items your audience can immediately put into practice where possible.

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.