Australian Government
Office of the Australian Information Commissioner

Privacy Management Plan

Office of the Australian Information Commissioner

15 December 2025 to 15 December 2026

Background

What is a Privacy Management Plan?

Australian Government Agencies are required to have a Privacy Management Plan (PMP) under the Australian Government Agencies Privacy Code. The PMP identifies specific, measurable privacy goals and targets and sets out how the agency will meet its compliance obligations under APP 1.2. The agency must measure and document its performance against its privacy management plan at least annually.

Before developing a PMP, the agency will need to understand the current state of its privacy practices. The OAIC has built on previous PMPs and used the OAIC's Interactive PMP Explained resource to help identify opportunities to improve maturity.

What are the next steps?

This PMP describes the actions that the OAIC will take in order to meet its privacy compliance obligations and maturity targets for the 2025/26 financial year. The OAIC PMP FY 25/26 builds on actions identified in previous PMPs and implemented to improve maturity levels. The PMP has a focus on innovative approaches to delivering PMP Compliance Activities.

About this PMP

Agency name	Office of the Australian Information Commissioner
PMP commencement date	Monday, 15 December 2025
PMP end date	Following its commencement, the Privacy Management Plan will remain in effect until it is superseded by a subsequent plan.
Recommended review period	Wednesday, 1 April 2026 to Monday, 30 June 2026

Privacy risk profile

While preparing this PMP, the OAIC has considered various matters relevant to its privacy risk profile. The details of these considerations are provided below for reference.

Privacy risk profile rationale	**Why the OAIC has a medium-to-high privacy risk?** The OAIC faces a medium-to-high level of privacy risk because we: • provide advice and guidance to other agencies/organisations on legislative requirements and best practice to comply with the Privacy Act. • oversee how other entities handle personal information under the Privacy Act and lead by example managing privacy complaints about OAIC. • collect and use personal information as part of our functions, specifically when investigating complaints, reviewing FOI decisions, and providing advice to the public. Information held by the OAIC can be very sensitive, especially when it involves people who are experiencing vulnerability.

- depend on public trust and confidence to perform our functions. People need to feel confident sharing their personal information with the OAIC so it can do its job properly. That trust is essential for the OAIC to work effectively.

Current state

Privacy maturity assessment outcomes

This PMP has been informed by an assessment of the OAIC's privacy maturity, the results of which are recorded in the table below.

The OAIC's overall privacy management maturity level rating is currently at 'defined' (based on the methodology set out in the Privacy Program Maturity Assessment Framework and outlined in the Interactive Privacy Management Plan Explained resource.)

Defined maturity level means Privacy culture is well developed and defined. Practices, procedures and systems are consistent, proactive, documented, integrated into broader organisational frameworks and measured.

Governance and Culture				
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**	**Activities to reach target level**
Privacy Champion	**Defined**	**Leader**	The OAIC's designated Privacy Champion is the Executive General Manager, Information Rights Division (EGM IRD). The Privacy Champion actively promotes good privacy practices across the agency. The Privacy Champion is a member of the OAIC Governance Board, providing accountability and executive oversight of privacy risks and promotes a culture of privacy that values and protects personal information. In this capacity, the EGM IRD speaks operationally and publicly on privacy and information matters. They have a mandate to drive improvements to uplift the OAIC's privacy culture.	Approving the PMP. Privacy Officers to incorporate quarterly updates on privacy risk and progress on PMP activities into Enabling Services Management Reports to Governance Board. Promotion of Privacy Champion at staff meetings and in staff communications.
Privacy Values	**Leader**	**Leader**	The OAIC meets the highest standard for promoting privacy. It shares its values publicly to show that protecting personal information is important. Each year, it runs Privacy Awareness Week to help OAIC staff and other agencies to understand why privacy matters. The agency values are reinforced in the introduction to the Governance Board Charter. *"The OAIC's purpose is to promote and uphold privacy and information access rights, and protection of personal privacy.* *The OAIC does this by ensuring proper handling of personal information under the Privacy Act 1988 (Privacy Act) and other legislation, protecting the public's right of access to documents under the Freedom of Information Act 1982 (FOI Act), carrying out strategic*	

Attribute	Current Level	Target Level	Rationale/Commentary	Activities to reach target level
			information management functions within Australian Government, and undertaking regulatory activities."	
Privacy Officer	**Defined**	**Leader**	The Privacy Officer for OAIC is in a unique position as it is the regulator and there is a heightened awareness and understanding about privacy requirements throughout the agency, and we continue to build on these strengths. We have established procedures and continually review processes for improvement to support the OAIC's work in privacy complaints and risk against the OAIC. The Privacy Officer also encourages privacy awareness.	Privacy Officers in Enabling Services will conduct an end-to-end review of privacy practice, procedures and systems and consider the effectiveness of broader integrated organisational frameworks.
Management & Accountability	**Defined**	**Leader**	The OAIC is in a unique position as it is the regulator and there is a heightened awareness and understanding of privacy requirements throughout the agency. The OAIC's purpose is to promote and uphold privacy and information access rights. We have regulatory responsibilities for privacy under the Privacy Act and other laws which include considering complaints and taking action in response to breaches of privacy of individuals. Responsibility for privacy compliance is vested in all officers and is given senior oversight in the agency. The management of the OAIC's privacy compliance practices is the responsibility of the Enabling Services Branch (for example, coordinating enquiries, complaints, access and correction requests). The OAIC publishes its Executive structure. The OAIC also publishes information about how to make a privacy complaint to the agency both in its agency capacity and as a regulator.	Investigation of the creation of a privacy database. Provide the Privacy Champion with fortnightly reports on privacy compliance prepared for the Agency Head. Updates on privacy compliance, risk and progress on PMP activities provided as part of the Enabling Services Management Reports to Governance Board.

Attribute	Current Level	Target Level	Rationale/Commentary	Activities to reach target level
			The OAIC's privacy compliance and performance, including progress on improvement initiatives, is reported monthly and quarterly to the Governance Board, and fortnightly to the Privacy Champion and the Agency head.	
Awareness	Leader	Leader	The OAIC aspires to meet the highest standard for promoting privacy. Staff have a strong awareness of privacy legislation and the Australian Government code. We provide mandatory annual training and promote awareness and compliance through other mechanisms regularly (such as the OAIC weekly newsletter to all staff, and emails from the CPO). The OAIC convenes Privacy Awareness Week annually to help OAIC staff and other agencies and APP entities to understand their obligations and educate the community on why privacy matters. These agency values are reinforced through the OAIC the Governance Board Charter.	OAIC Privacy Officers are exploring innovative ways to promote privacy awareness through a whole of compliance training and information suite, including 3-minute training videos that encompass privacy awareness. Enliven the Compliance awareness pack utilising the Commissioners strategic intent by aligning to the guiding principles outlined in the 4 Pillars (4Ps): - Proactive - Proportionate - Purposeful - People focussed

Privacy Strategy				
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**	**Activities to reach target level**
Privacy Management Plan	**Defined**	**Leader**	The agency has a published 24-25 PMP that is available on the OAIC website. The 25-26 PMP is being finalised and will be endorsed when completed. The CPO has considered resourcing to complete the activities in the PMP. The activities have been designed to build on and progress privacy maturity outcomes in the changing environment.	Privacy Officers to incorporate quarterly updates on privacy risk and progress on PMP activities into Enabling Services Management Reports to Governance Board. The OAIC's Privacy Management Plan 2025-2026 will be published on the OAIC website.
Inventory of Personal Information	**Defined**	**Leader**	The OAIC stores personal information in the Resolve database system and Content Manager. Details about how the OAIC collects, uses, and discloses personal information to exercise its powers and perform its functions are outlined in the OAIC Privacy Policy, available on the OAIC website. The OAIC has a PIHR and understand a data flows in and out of the agency. This includes: - Resolve - CDR - Content Manager - Outlook - ERP (SAP HR) The overarching Records Management Framework encompasses all personal information within the Information Governance Framework Records monitors our PIHR.	Further mapping of personal information holdings in OAIC systems will be conducted (Resolve, Hub, ERP). An evaluation of Content Manager practices will also be undertaken to promote automated alignment with retention and disposal authorities aligning with NAA standards. Each system will be evaluated to ensure appropriate classification and capture systems are in place – this includes consideration of Microsoft Teams functionality.

Attribute	Current Level	Target Level	Rationale/Commentary	Activities to reach target level
Data Quality Processes	**Defined**	**Leader**	OAIC staff are aware of their privacy obligations and the need to ensure that action is taken to correct and update personal information records where appropriate. The OAIC also has strict retention and destruction policies which complement its data quality processes (see the OAIC's Disposal Authority for more information). The OAIC routinely takes opportunities to enhance its processes for ensuring the accuracy of the personal information records it collects and holds when performing its functions. The OAIC promotes data quality practices across the public and private sectors through resources published on its website, in handling complaints and undertaking other regulatory action. and audits are conducted on an ongoing basis.	Privacy training is regularised throughout the OAIC and will include guidance on data quality.
Information Security Processes	**Defined**	**Defined**	OAIC has an established information-security aware culture. There is dedicated mandatory induction and annual refresher training on Security and Privacy for all OAIC staff. Periodic reminders are also issued on staff obligations to adhere to required security policies including ICT use and information (need to know) access. The OAIC CIO works with DEWR on phishing campaigns to increase staff awareness on cyber security risks. Staff have access to guidance materials and training to ensure an understanding of privacy and security obligations,	The OAIC will continue to promote information security and to review related guidance, policy and processes with a particular emphasis on staff on-boarding and off boarding. Enliven the Compliance awareness pack using the Commissioners and aligning with the 4 Ps: - Proactive - Proportionate - Purposeful - People focussed Incorporate small videos for intranet (3mins) on Security and other compliance activity.

Attribute	Current Level	Target Level	Rationale/Commentary	Activities to reach target level
			policies and processes. The OAIC's Cyber Security Response Plan, which was designed to integrate risk with the Data Breach Response Plan, also operates alongside these frameworks. The OAIC's information systems are managed under a shared services arrangement with DEWR. The OAIC does share its knowledge in relation to privacy and information security with other agencies through its regulatory role. Where possible, the OAIC collaborates with other agencies on its own information security processes, including the sharing of risk assessments as required by PSPF Direction 4-0225.	Reintroduce a program of spot checks on Resolve access.

Privacy Processes				
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**	**Activities to reach target level**
External Privacy Policy & Notices	**Leader**	**Leader**	Privacy messaging is viewed as an opportunity to build trust and engage the public. The OAIC holds the annual Privacy Awareness Week and uses the opportunity to delivery privacy education to the public using a variety of techniques (infographics, animation, games, videos, webinars, speeches). The OAIC privacy policy, privacy policy summary and human resources privacy policy are publicly available on the OAIC website.	
Internal Policies & Procedures	**Defined**	**Leader**	The agency has a comprehensive Privacy Policy that is available to the public. The Policy sets out the key points about how the OAIC handles personal information. The OAIC regularly reviews and updates internal process/policy documents due to changing environments.	The OAIC will monitor outcomes of the Governance Board decision making regarding privacy management to inform the quarterly review of our action plan and privacy policies.
Privacy Training	**Defined**	**Leader**	The OAIC provides all staff with privacy training including mandatory induction training and mandatory annual refresher training. OAIC training has been designed in house and is more comprehensive than the standard APSC training. The OAIC monitors staff compliance with their training requirements. Mandatory individual learning is an essential requirement for all OAIC staff to ensure we meet our obligations under several laws and	The new OAIC intranet provides access to additional resources and training opportunities including new 3 minute videos. Updates on guidance, training opportunities and agency policies will also be circulated via

Attribute	Current Level	Target Level	Rationale/Commentary	Activities to reach target level
			includes induction and mandatory training. It also ensures that we work within robust governance and risk frameworks. The OAIC also guides staff to additional training, specifically the APSC privacy modules, and encourages them to undertake this training as well. Further specific training is provided to staff based on their role in the agency – for example, intake and eligibility staff and privacy case management staff in the Information Rights Division receive additional training specific to their roles in handling privacy complaints and notifiable data breaches.	weekly wrap all staff newsletter. The Privacy training module to be reviewed by April 2027 to ensure the content is still relevant. Privacy awareness pack reviewed to ensure alignment with the 4 Ps: - Proactive - Proportionate - Purposeful - People focussed
Privacy Impact Assessments	**Defined**	**Leader**	While the OAIC is continually navigating rapid technological changes and evolving expectations of government in service delivery, the principle of privacy remains constant. The OAIC has developed internal PIA guidance that is engaging and user-friendly. The internal guidance includes links to external-facing guidance and resources, including tools and templates, on the OAIC website. Privacy by design principles are applied consistently across the OAIC with express consideration to privacy impacts embedded in project and Executive brief templates	The OAIC Privacy Officers will conduct an end-to-end review of the PIA procedures due to a current restructure.
Dealing with Suppliers	**Leader**	**Leader**	The OAIC uses Whole of Government standard contracts within the Commonwealth Contracting Suite (CCS) as required by the Commonwealth Procurement Rules (CPRs) to	

Attribute	Current Level	Target Level	Rationale/Commentary	Activities to reach target level
			comply with Section 15 of the Public Governance, Performance and Accountability Act 2013 (PGPA Act). The CCS has been developed to ensure compliance with CPRs and PGPA as standard templates across government. The CCS includes standard terms including privacy and confidentiality clauses. It also includes the ability to add in specific clauses for privacy and confidentiality that can be customised based on the requirements of a specific contract. The OAIC undertakes relevant assessments and audits of third party suppliers where privacy and confidentiality are central to the procurement process where necessary.	
Access & Correction	**Defined**	**Leader**	The OAIC routinely gives individuals access to their personal information pursuant to statutory mechanisms including via administrative access and requests made under APP 12 and APP 13 of the Privacy Act. The OAIC internal policy and procedures guide staff in how to process these requests in accordance with the relevant framework. It consciously undertakes to be responsive, open and transparent in its dealings with access and correction requests.	The OAIC will review internal guidance for staff on administrative access and APP 12 requests.
Complaints & Enquiries	**Defined**	**Leader**	Complaints made to the OAIC about its conduct in relation to the collection and handling of personal information are received and managed by the Enabling Services Branch. OAIC publishes	Finalise a comprehensive guide for staff.

Attribute	Current Level	Target Level	Rationale/Commentary	Activities to reach target level
			its policy and process for complaints about OAIC employees or contractors on its website to ensure the public is aware of the OAIC's complaints and handling processes.	Investigate a dedicated resolve process for OAIC privacy activity and reporting.

Risk Assurance				
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**	**Activities to reach target level**
Risk Identification & Assessment	**Defined**	**Defined**	The OAIC has strong, clear and consistent processes to identify and assess privacy risks as part of its PIA and risk management policies and procedures. All initiatives involving new ways of handling personal information are assessed for privacy risk as part of the PTA and PIA processes and are reported to the Executive and Chief Privacy Officer in a timely manner. Privacy risk is acknowledged as part of all business activity and risk management strategies are used to manage perceived or actual risks.	Review the Risk Management Policy and Framework to further integrate privacy risk within the Agency Risk Framework.
Reporting & Escalation	**Defined**	**Defined**	The OAIC promotes a positive risk culture in which staff at every level appropriately manage risk as part of their day-to-day work. The OAIC's PIAs, PMPs and review of internal processes are endorsed by the agency's Privacy Champion. OAIC has an escalation and reporting process, providing a framework for reporting on privacy incidents and complaints to senior management. Privacy Executive Reports are presented to the Agency Head fortnightly and monthly privacy reports are provided to Governance Board.	Privacy Officers to incorporate quarterly updates on privacy risk and progress on PMP activities into Enabling Services Management Reports to Governance Board and privacy risks are reported to Audit and Risk Committee.

Attribute	Current Level	Target Level	Rationale/Commentary	Activities to reach target level
Assurance Model	**Developing**	**Defined**	All staff have responsibility for identifying and escalating privacy issues, including to the Privacy Officers/CPO. Reports are provided to the agency head fortnightly, and Governance Board monthly. The Privacy Officers/CPO provides guidance, collaborates with information security, data governance and risk functions to identify opportunities and best practice and continuous improvement.	The procedures for reporting will be reviewed.

Data Breach Response				
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**	**Activities to reach target level**
Data Breach Response Plan	**Defined**	**Leader**	The OAIC has a Data Breach Response Plan (DBRP) with clear and documented roles and escalation paths which is published on its website. The DBRP has been integrated with other business critical functions including information technology and physical security. The DBRP is accessible to all staff and agency-wide emails have been used to build awareness of how to recognise a data breach and apply the plan.	The OAIC will conduct an end-to-end review of the DPRB procedures and test the regime of the plan.
Data Breach Notification	**Leader**	**Leader**	The OAIC's DBRP sets out the relevant process and has a heightened understanding of the Eligible Data Breach Scheme.	