Australian Government
Department of Education

Inquiry into the management of client privacy in the Australian public sector

Submission from the Department of Education to the Joint Committee of Public Accounts and Audit

Contents

Inquiry into the management of client privacy in the Australian public sector

Introduction

1. The Department of Education (the department) makes the following submission to the Joint Committee of Public Accounts and Audit (the Committee) on its inquiry into the management of client privacy in the Australian public sector.

2. The department understands that, as part of this inquiry, the Committee will examine:

    - the frameworks used to identify and manage privacy risks, and meet the requirements of the *Privacy Act 1988* (Privacy Act), in public sector entities that manage information on private individuals

    - the ability of public sector entities holding personal information to respond effectively to data breaches, cyber threats, and malicious actors, and

    - any matters contained in and associated with Auditor-General Report No. 12 of 2025–26: Managing the Privacy of Client Information in Services Australia.

3. The department is responsible for national policies and programs that help Australians access quality and affordable child care, early childhood education, school education, post school higher education, international education and academic research. The department is a policy agency that handles some client personal information, including sensitive information. However, the department handles less personal information than some other agencies that provide complex public services.

4. The department has a range of measures in place to ensure it complies with relevant privacy obligations and appropriately manages and protects the personal information it holds. A brief overview of those arrangements, including privacy governance frameworks, is outlined below.

The department's arrangements to manage privacy

Governance and oversight arrangements, including reporting

5. In accordance with the *Privacy (Australian Government Agencies – Governance) APP Code 2017* (Privacy Code), the department has appointed a Privacy Champion and has two Privacy Officers. The Privacy Officers sit within the Corporate and Information Law Team (CIL Team) in the Legal Division. The CIL Team is responsible for privacy policy and advising on the Privacy Act in the department. This includes providing advice on internal and external privacy enquiries, privacy complaints and other privacy incidents.

6. The Privacy Code also requires the department to ensure that certain privacy functions are carried out, one of which is to provide regular privacy reports to the department's Executive, including about any issues arising from the department's handling of personal information.

7. In accordance with this obligation, and for the purposes of ensuring the department's Executive has appropriate oversight of privacy incidents involving the department, the Privacy Champion briefs the department's Executive annually on the department's performance in relation to privacy. This briefing, referred to as the Annual Privacy Review Report, is provided to the department's Executive at the end of each financial year.

8. The Annual Privacy Review Report covers matters such as:
    - incidents involving the department that have been reported to the CIL Team within the relevant reporting period, including:
        - privacy incidents that have been assessed to be eligible data breaches for the purposes of the Privacy Act
        - other significant privacy incidents and complaints, including those indicating any systemic issues
        - significant privacy incidents arising from other agencies or third parties and involving the department
    - key privacy actions taken during the relevant financial year, including the department's performance against its Privacy Management Plan, and
    - any broader privacy issues affecting the department.

9. In addition to the above, the department's Privacy Champion provides regular privacy updates to the department's Audit and Risk Committee. This includes a report on any privacy incidents received in the relevant reporting period and outlines whether any significant or systemic issues have been identified.

10. The department also has in place a Privacy Reporting Protocol, approved by the department's Executive Board, that sets out roles and responsibilities for the reporting of privacy incidents, including breaches and complaints. This assists in ensuring that the department's Executive is briefed in a timely manner about privacy matters.

Policies to manage the privacy of client information

11. The department has in place key privacy policies, including:
    - Privacy Policy
    - Data Breach Response Plan
    - Privacy Impact Assessment (PIA) Policy
    - Privacy Complaints Handling Procedures

12. These policies are complemented by a range of associated policies, plans and registers such as:

- Privacy Management Plan
- Personal Information Holdings Register
- Privacy Impact Assessment Register
- Information Management Policy
- Data Release, Sharing and Use Policy
- Handling and Storing Classified Information Policy
- Information Retention and Disposal Policy

13. There are also a range of privacy related guides, templates and fact sheets available to staff on the department's intranet that are designed to assist staff appropriately manage the privacy of client information. Additionally, many business areas have their own specific policies and procedures that govern the handling of information, including to ensure compliance with any applicable secrecy provisions in the department's portfolio legislation that sit alongside any Privacy Act obligations.

Education and training arrangements

14. The department provides privacy training as part of its induction program. Additionally, as part of the department's ongoing mandatory training program, all staff are required to undertake annual privacy awareness training. Completion of this training is monitored and tracked.

15. The CIL Team also proactively offers and provides tailored privacy training to business areas, for example, in response to issues relating to a business area's handling of personal information, or as requested by a business area.

16. The Privacy Champion and/or the CIL Team distribute privacy messages and articles to departmental staff, particularly where staff need to be made aware in a timely way of any emerging issues or privacy reforms.

17. The Privacy Champion and CIL Team actively promote Privacy Awareness Week, which is an annual initiative led by the Office of the Australian Information Commissioner (OAIC). During the week, staff are encouraged to participate in the range of privacy activities made available, including quizzes, presentations, and articles.

Implementation of arrangements to manage the privacy of client information

Privacy Impact Assessments

18. The department has a PIA Policy, which sets out the procedures, roles and responsibilities for conducting Privacy Threshold Assessments and PIAs in the department as part of the department's broader risk assessment and change management processes. The PIA Policy also includes information about roles and responsibilities for ensuring the department's PIA Register is maintained consistent with

the department's obligations under the Privacy Code. In accordance with the department's Accountable Authority Instructions (AAIs), officials in the department are required to comply with the PIA Policy.

Privacy Management Plan

19. The department has a Privacy Management Plan (PMP) in place which identifies specific, measurable privacy goals and targets, and sets out how the department will meet its compliance obligations under Australian Privacy Principle (APP) 1.2 and the Privacy Code for the relevant financial year.

20. The department's performance against the PMP is measured and documented annually as required under subsection 9(3) of the Privacy Code. The department has developed its PMP with reference to the OAIC's 'Interactive PMP template' and 'Interactive PMP Explained' resource, including the Privacy Program Maturity Assessment Framework at Appendix 1 of that resource.

Monitoring of privacy incidents and complaints

21. In addition to the reporting frameworks discussed above, the department's Data Breach Response (DBR) Plan sets out the process, roles and responsibilities for managing an actual or suspected data breach involving personal information. In accordance with the department's Accountable Authority Instructions (AAIs), officials in the department are required to comply with the DBR Plan.

22. The DBR Plan helps ensure that suspected or actual data breaches are handled by the department consistently with its obligations under the Privacy Act and in a timely manner to minimise harm to any affected individuals. Relevantly, the DBR Plan ensures that key personnel are made aware of the matter, including the department's Privacy Officers, IT Security Advisor and Agency Security Advisor.

23. The department tracks incidents reported to the Privacy Officers and this data is used to ensure:

    - individual incidents are assessed as required under the Privacy Act
    - appropriate reporting occurs, including so relevant business areas and the Executive have oversight of privacy incidents and matters
    - any trends or significant or systemic privacy issues are identified, and
    - privacy or security controls are strengthened where any gap is identified.

24. The department's AAIs also require officials to consult with the Privacy Officer before responding to any complaint from an individual that the department has interfered with the individual's privacy. Privacy complaints are similarly tracked and reported on as appropriate.

Number of notifiable data breach since 2022-23 financial year

25. Since 1 July 2022, the department has been involved in one notifiable data breach as per the data breach scheme set out in Part IIIC of the Privacy Act. The data breach occurred in April 2023 when one of the department's contracted legal service providers was the target of a malicious cyber incident involving personal information being exfiltrated from its IT systems and made available on the dark web. The data breach was identified by the relevant provider, which notified the department that some jointly held personal information was involved in the cyber incident.