audit office
OF NEW SOUTH WALES

Privacy Management Plan

Date: 27 March 2024

contents

1. Introduction 1
2. About the Audit Office 1
3. Legislative framework 1
4. Policy and procedure development and review 2
5. Implementing and promoting the Plan 2
5.1 Audit Office staff 2
5.2 Public awareness 3
6. The Privacy Officer 3
7. How the Audit Office manages personal information 3
7.1 Functions of the Audit Office 3
7.1.1 Audit and audit-related functions 3
7.1.2 Corporate function 3
7.2 Collection 4
7.3 Storage 8
7.4 Access, accuracy and use 9
7.5 Disclosure 11
8. Breaches of the PPIP Act and the HRIP Act 13
8.1 Data Breach Management Policy 13
9. Review rights and complaints 13
9.1 Complaints 13
9.2 Internal review 13
9.3 External review by the NSW Civil and Administrative Tribunal (NCAT) 14
9.4 Complaints to the Privacy Commissioner 14
10. Contacting the Audit Office 14
11. Review 14
Document information 15
Document history 15
Appendix 1 – About NSW's privacy laws 16
1. The PPIP Act and personal information 16
1.1 About personal information 16
1.2 Information protection principles (IPPs) 16
1.3 Exemptions to the IPPs 17
1.4 Offences 17
1.5 Public registers 17
2. The HRIP Act and health information 18

2.1 About health information 18
2.2 Health privacy principles (HPPs) 18
2.3 Exemptions to the HPPs 19
2.4 Offences 19
Appendix 2: Other applicable laws 20
2.1 GSA Act 20
2.2 LG Act 20
2.3 Crimes Act 20
2.4 GIPA Act and GIPA Regulation 20
2.5 ICAC Act 20
2.6 PID Act 21
2.7 State Records Act and State Records Regulation 21
Appendix 3: Audit Office privacy-related policies 22

1. Introduction

The Audit Office of New South Wales (the Audit Office) is required by section 33 of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) to have and implement a Privacy Management Plan (the Plan). This Plan includes information on the type of personal information[1] the Audit Office holds, details on how people can access their personal information and what they can do if they think the Audit Office has breached the PPIP Act.

2. About the Audit Office

The Audit Office is a statutory authority, established under the *Government Sector Audit Act 1983* (GSA Act), that conducts financial and performance audits for the Auditor-General.

The Audit Office conducts financial and performance audits of NSW Government agencies, universities and local councils, principally under the GSA Act and the *Local Government Act 1993* (LG Act).

These audits help parliament hold government accountable for its use of public resources.

Further information about the functions of the Audit Office is contained in the Audit Office Information Guide available on our website.

3. Legislative framework

The PPIP Act sets out the responsibilities of public sector agencies, including the Audit Office, in respect of the management of personal information. Division 1 part 2 of the PPIP Act contains 12 Information Protection Principles (IPPs) which cover the key areas of:

- collection
- storage
- access and accuracy
- use
- disclosure of personal information.

In 2023, amendments to the PPIP Act introduced a mandatory data breach notification scheme. This requires the Audit Office to notify individuals and the Privacy Commissioner when there are data breaches of personal information that are likely to result in serious harm to the individual. For more information, see the Audit Office's Data Breach Management Policy.

In addition to the PPIP Act, the *Health Records and Information Privacy Act 2002* (HRIP Act) contains specific provisions about the management of health information and includes a set of Health Privacy Principles (HPPs).

Appendix 1 contains the definitions of personal and health information and a summary of IPPs and HPPs as they apply to the Audit Office.

Other legislation affecting the way in which the Audit Office manages information includes:

- *Government Sector Audit Act 1983* (GSA Act)
- *Local Government Act 1993* (LG Act)
- *Crimes Act 1900* (Crimes Act)
- *Government Information (Public Access) Act 2009* (GIPA Act)
- *Government Information (Public Access) Regulation 2018* (GIPA Regulation)
- *Independent Commission Against Corruption Act 1988* (ICAC Act)
- *Public Interest Disclosures Act 2022* (PID Act)
- *Public Interest Disclosures Regulation 2022* (PID Regulation)
- *State Records Act 1998* (State Records Act)

- *State Records Regulation 2015* (State Records Regulation).

Appendix 2 contains additional information about these acts and regulations.

4. Policy and procedure development and review

To ensure compliance with the requirements of section 33(2) of the PPIP Act, the Audit Office is required to set out in this Plan how policies and practices are developed and implemented. This Plan sets out a number of specific elements of the Audit Office's privacy protection framework. Policies and procedures to guide implementation are developed by:

- examining changes in the legislative, policy or operational environment for their impacts on the privacy management of the Audit Office
- conducting regular reviews of privacy policies including reviews against guidance published by the Information and Privacy Commission (IPC)
- considering the privacy implications of changes to policies and systems for any procedural changes needed.

When developing new privacy management policies or procedures or amending them in a way that would change how personal information is managed, the Audit Office consults with the applicable parties to ensure compliance with the PPIP Act and the HRIP Act.

Appendix 3 contains a list of Audit Office privacy related policies.

5. Implementing and promoting the Plan

The Audit Office reinforces transparency and compliance with the PPIP Act and the HRIP Act by:

- endorsing the Plan and making it publicly available
- ensuring the Plan is regularly reviewed and updated as appropriate
- ensuring associated policies and plans are developed, implemented, and regularly reviewed, including a data breach management policy and plan for the implementation of mandatory notification requirements
- reporting on privacy issues in the Audit Office annual report in accordance with the *TPG23-10 Annual Reporting Requirements*
- undertaking an annual self-assessment of compliance with the PPIP Act
- confirming support for privacy compliance in the Audit Office's Code of Conduct
- endorsing a culture of good privacy practice
- identifying privacy issues when implementing new systems
- reporting privacy breaches to the Office Executive and the Audit and Risk Committee.

5.1 Audit Office staff

The Audit Office is committed to making staff aware of their privacy obligations and promoting awareness of privacy obligations among staff by:

- publishing the Plan, privacy related policies and other information about privacy on the intranet
- including a reference to the Plan in the onboarding form as part of the induction process
- proactive reporting of any identified privacy breaches or risks to the Privacy Officer (the Director, Governance (Legal))
- providing specialist advice and guidance on privacy issues to staff when required
- providing updates to staff on changes to the legislation and key developments in the field.

5.2 Public awareness

This Plan provides information to members of the public about how the Audit Office manages personal information. The Audit Office promotes public awareness of the Plan by:

- writing the Plan in plain English
- publishing the Plan on the Audit Office website in accordance with the open access provisions of the GIPA Act
- informing people about the Plan when responding to enquiries about personal information.

6. The Privacy Officer

The Privacy Officer for the Audit Office is responsible for this Plan and any associated policies and procedures that help the Audit Office meet its obligations under the PPIP Act and the HRIP Act.

The Privacy Officer is the first point of when privacy issues arise, either internally or externally, and has responsibility for ensuring that Audit Office privacy policies and procedures are fully implemented.

7. How the Audit Office manages personal information

7.1 Functions of the Audit Office

7.1.1 Audit and audit-related functions

The Audit Office maintains the confidentiality of all information obtained whilst undertaking audit and assurance work. Exceptions include the Auditor-General's Report to Parliament and where the office is required to disclose information under section 38 of the GSA Act and section 425 of the LG Act.

The Audit Office may receive personal or health information about individuals from an agency being audited as part of the audit process.

Personal information obtained during the audit process is covered in section 27A(b)(iii) of the PPIP Act. This section provides that a public sector agency is not required to comply with the IPPs with respect to the collection, use or disclosure of personal information if the information is being exchanged between public sector agencies to enable the auditing of the accounts or performance of a public sector agency. Clause 10(1)(b) of Schedule 1 to the HRIP Act enables an entity to disclose health information to the Audit Office for the purposes of auditing the provision of a product or services the organisation has provided or is providing to the person.

Outside of this exemption concerning the transfer of information between public sector agencies, information received by the Audit Office is managed in accordance with the IPPs of the PPIP Act and the HPPs of the HRIP Act.

The Audit Office's internal guidance provides information and examples to audit teams to assist in the compliant collection, storage, management, use and disclosure of personal and health information.

7.1.2 Corporate function

When carrying out the corporate functions, the Audit Office receives personal and/or health information about individuals such as staff, contractors, consultants, visitors and members of the public. The Audit Office complies with the PPIP Act and the HRIP Act in the way it manages personal and health information obtained as part of the corporate functions.

7.2 Collection

Requirement on the AO	Audit function	Corporate function
IPP 1 Section 8 of the PPIP Act – information must only be collected for a **lawful purpose** directly related to the agency's functions or activities and be **reasonably necessary** for that purpose. **HPP 1** Schedule 1 of the HRIP Act – information must only be collected for a **lawful purpose** directly related to the agency's functions or activities and be **reasonably necessary** for that purpose.	The Audit Office only collects personal information for a lawful purpose to support the conduct of financial and performance audits. Personal information collected during the audit process may include names, contact details, payroll information, employment details and details of contractual arrangements between individuals and agencies. If health information is collected during the audit process, the nature of the information collected depends on the nature of the audit. The Performance Audit Guide, for example, states that personal and health information should be requested and provided in de-identified forms. The Audit Office does not routinely collect health information about members of the public.	The Audit Office only collects such information as is reasonably necessary to fulfil its corporate functions. The primary purpose for collecting personal information is to enable the processing of employment applications and managing the ongoing employment relationship, such as maintaining employee records and administering employment, salary and superannuation. **Ways the Audit Office collects or holds personal information** 1. Recruitment and employment records: • documents related to the recruitment process, including education and employment history • personal contact details and emergency contact details (phone number, postal and email address) • date of birth • financial information (such as salary, bank account information, tax file number, superannuation fund details) • personnel information (such as payroll, attendance and overtime records, leave balances, educational and professional qualifications, training and development records) • sensitive background information (such as criminal history, ethnic background, disability) • performance reviews and development plans. 2. Conflict of Interest and Professional Independence Register 3. Office Executive Conflict of Interest Register 4. Remuneration Committee Conflict of Interest Register 5. Audit and Risk Committee Conflict of Interest Register 6. Secondary Employment and Volunteering Register 7. Information about visitors to the Audit Office: An electronic visitor sign-in system, displayed on the front counter in the reception area, is used to record names and contact details (phone number or email) of people who enter the office. The system includes a link to this Plan. The Audit Office collects the visitor information for workplace health and safety purposes. 8. Information collected for mailing lists – name and email. 9. Information collected for client and parliamentary surveys – name and contact details, including email, phone number, position, organisation details.

Requirement on the AO	Audit function	Corporate function
		10. Visits to the Audit Office website, see the website Privacy Policy for more information. 11. Information collected as part of GIPA Act access applications and requests for information – name, contact details and other personal information specific to a particular matter. 12. When receiving public interest disclosures under the PID Act (reports may be public officials of the Audit Office, or of another agency), and when receiving complaints and feedback from members of the public about the entities the Audit Office audits. PIDs, complaints and feedback can be anonymous but usually contains personal information about the person making them (such as contact details, personal opinions, stories, experiences and backgrounds) and may also contain personal information about a third party, or about the office itself Section 4(5) of the PPIP Act and section 10 of the HRIP Act provide that personal information and health information, respectively, is not 'collected' by a public sector agency if the receipt of the information by the agency is unsolicited (as with PIDs, complaints and feedback). This means the Audit Office is not required to comply with the IPPs and HPPs on the collection of such information. In circumstances when a PID, complaint, feedback or other enquiry is received via a phone call, the Audit Office phone will display the number of the person who called, except for silent numbers. Phone conversations are not electronically recorded. If someone has an enquiry that cannot be answered straight away, a receptionist will offer to take the person's name and phone number and will forward the enquiry, along with the contact details, to an appropriate staff member to respond. 13. Occasionally, the Audit Office will receive information from other integrity agencies, including when referred to the Audit Office in accordance with the Memoranda of Understanding. See part 7.6 of this Plan for further information on referrals from other agencies. 14. The Audit Office collects **health information** about staff including: • medical certificates • health declarations showing medical conditions • fitness for duty assessments[2] • workers compensation records • workplace health and safety records • other medical information

[2] Fitness for duty assessments are conducted by an independent medical assessor. The assessor provides a report to the Audit Office. The affected employee is aware that a report is provided to the Audit Office and also receives a copy. The information in the report is treated in accordance with the PPIP Act and the HRIP Act.

Requirement on the AO	Audit function	Corporate function
IPP 2 Section 9 of the PPIP Act – information must be collected **directly** from the individual. **HPP 3** Schedule 1 of the HRIP Act – information about an individual must be collected from the individual concerned.	Any personal or health information collected during an audit is collected from the agency being audited – see section 27A(b)(iii) of the PPIP Act.	In most circumstances personal and health information is collected directly from the individual e.g., the employee. For example, information in the online recruitment application and in the onboarding form, or medical information submitted by an individual as part of a personal leave application. In some circumstances information about employees may be provided by third parties, such as third- party recruitment providers, previous employers and nominated referees.
IPP 3 Section 10 of the PPIP Act – take reasonable steps to ensure the individual is **aware** information is being collected and **why**. **HPP 4** Schedule 1 of the HRIP Act –take reasonable steps to ensure the individual is **aware** information is being collected and **why**.	Not applicable – see references to exemption for the audit function above.	Personal information is collected during the online recruitment process and subsequently further personal information (such as bank details, superannuation fund details etc.) is collected from successful applicants in the onboarding form. New starters are told why their personal information is collected and how it will be used. The personal information collected is handled in accordance with this Plan. The onboarding form includes questions relating to equal employment opportunity data collection. This section contains questions on sensitive personal information, such as racial and cultural information. Providing this information is voluntary. Information relating to applicants who meet the requirements for an eligibility list is retained by the Audit Office in the selection committee report. Information relating to unsuccessful applicants is stored in the online recruitment portal. Successful applicants receive an offer letter which includes a statement that the Audit Office provides details of their employment to the Public Service Commission, and that the information is provided in a format that maintains privacy. Health information in relation to disability status is collected during the recruitment process for the purpose of identifying if any adjustments need to be made during recruitment.. Employees complete a health declaration at the onboarding stage or at other times if they consider doing so is useful for the Audit Office to make reasonable adjustments to working arrangements.

Requirement on the AO	Audit function	Corporate function
IPP 4 Section 11 of the PPIP Act – take reasonable steps to ensure the information collected is **relevant, accurate**, complete, up to date, **not excessive** and not an unreasonable intrusion. **HPP 2** Schedule 1 of the HRIP Act - take reasonable steps to ensure that the information collected is **relevant**, not excessive, **accurate**, up to date, complete and **not an unreasonable intrusion**.	The Audit Office collects personal information from audited agencies to support the conduct of financial and performance audits. The Audit Office relies on the agency providing the audit information to confirm its accuracy, currency, and completeness.	The Audit Office takes reasonable steps to ensure that information collected from individuals is not unreasonably intrusive or excessive, and is relevant, accurate, up-to-date and complete. For example, in collecting information from new starters as part of the onboarding process, the Audit Office only asks for information that is necessary to perform our function as an employer e.g. contact details, emergency contact details, tax file number etc. Staff can view and update their personal information using online systems. Employees are required to complete a health declaration at the onboarding stage or on as needs basis in the context of making reasonable workplace adjustments. Often the full disclosure of health status or medical conditions is not required for reasonable workplace adjustments to be made.

7.3 Storage

Requirement on the AO	Audit function and corporate function
IPP 5 Section 12 of the PPIP Act – information must be **stored securely**, kept no longer than necessary and **disposed of appropriately**. **HPP 5** Schedule 1 of the HRIP Act – information must be **stored securely**, kept no longer than necessary and **disposed of appropriately**.	The Audit Office has a number of policies in place (available on the intranet) to ensure that personal and health information is stored, retained and disposed of appropriately including: Records Management Policy • Secure Desk and Documentation Policy • Office Access Policy • Information Security Policy • Information Security Management System Framework (ISMS Framework) • Backup and Archiving Policy • Secure Deletion and Disposal Policy. Records containing personal and health information are retained in accordance with the retention and disposal authorities made under the State Records Act. Most of the personal and health information collected or held by the Audit Office is stored electronically. Personnel files for employees containing personal and health information are only accessible by relevant staff within the Audit Office's People & Culture function, and available to direct managers on an as needs basis on the consent of the employee. The Audit Office Information Security Policy and the (website) Privacy Policy apply to the personal information held electronically. The majority of the hard copy files are archived in an off-site secure storage facility in compliance with the State Records Act. Occasionally, some hard copy files are recalled from the storage facility. During this time, they are securely stored in the Audit Office at Level 19, Darling Park Tower Two, 201 Sussex Street, Sydney NSW 2000. Once processed, they are transferred back to the storage facility, or if appropriate, destroyed using the secure destruction facilities (secure lockable bins). Other personal and health information is stored outside the office, for example when engaging a third party to host and manage an information system or storing data in the cloud. Before storing information in new locations, the Audit Office will complete a privacy impact assessment. For IT related systems, this may also include undertaking an IT security risk assessment. In addition, when engaging a third party, privacy obligations are to be included in contractual arrangements.

Requirement on the AO	Audit function and corporate function	
IPP 5 Section 12 of the PPIP Act – information must be **protected** from unauthorised access, use, or disclosure. **HPP 5** Schedule 1 of the HRIP Act – information must be **protected** against loss, unauthorised access, use, modification, disclosure, and misuse.	Personal or health information collected during an audit is stored in electronic audit files. Only authorised staff members have access to these files.	The Audit Office records management system contains restrictions and controls to make sure that personal and health information stored electronically can only be accessed by authorised staff. All of the Audit Office electronic information is stored securely. The system complies with the international Information Security Standard ISO 27001:2013 as per the ISMS Framework. Staff access to the network is restricted by an individual user ID and password. The Audit Office Secure Desk and Documentation Policy, which applies when employees work at 201 Sussex Street, at client sites, when working from home, or in any other physical space where work on behalf of the Audit Office takes place, provides for 'a clean desk' approach meaning hard copy files are secured at the end of the day and when not in use. All staff have access to personal secure lockers and lockable cabinets. Files and working papers are secured in locked lockers or cabinets after hours and during business hours when not in use, they are not left on desks or in other open areas. Files and working papers are only accessible by the employees requiring them for the completion of specific duties. Drafts, spare copies and extra materials generated in the handling of files and working papers that are deemed not to be an Audit Office record are to be destroyed by means of Audit Office's secure destruction facilities. Audit Office staff have security access cards to enter the office. Visitors cannot enter without permission.

7.4 Access, accuracy and use

Requirement on the AO	Audit function	Corporate function
IPP 6, IPP 7 and IPP 8 Sections 13 and 14 of the PPIP Act – must enable the individual to **find out** if information relating to them is held, and **how to access** it; allow **access** without excessive delay or expense; enable updates or corrections. **HPP 6, HPP 7 and HPP 8**	The Audit Office does not collect personal or health information directly from an individual during the audit process, rather it collects information from an agency. Any person wishing to access or amend their personal or health information which has been obtained by the Audit Office as part of an audit should	<u>Access</u> Everyone has the right to access and amend the personal and health information the Audit Office holds about them. The Audit Office will take reasonable steps to ascertain whether the Audit Office holds the information about an individual, the nature of this information, the purpose for which it is used and an individual's rights to access this information. The Audit Office is required to provide access to the personal and health information it holds and allow this information to be amended without excessive delay or expense. There is no fee to access or amend personal or health information. Contact the Privacy Officer to: • find out whether the Audit Office holds personal or health information about you • make an access request, or

Requirement on the AO	Audit function	Corporate function
Schedule 1 of the HRIP Act – must enable any individual to **find out** what health information related to them is stored**; reasons** for its use, and **how to access** it; allow **access** to without excessive delay or expense; enable updates or corrections**.** **IPP 9** Section 16 of the PPIP Act – the personal information must be **relevant**, **accurate**, **up to date, complete** and **not misleading**. **HPP 9** Schedule 1 of the HRIP Act – the health information must be **relevant**, **accurate**, **up to date**, **complete** and **not misleading**. **IPP 10** Section 17 of the PPIP Act – the personal information must be **used for a purpose it was collected** and its use is limited to that purpose. **HPP 10** Schedule 1 of the HRIP Act – the health information must be	contact the agency providing the information. The Audit Office relies on the agency providing the audit information to confirm its accuracy, currency, and completeness. Any personal and health information collected during the audit process is only used for the purpose of the audit. The audit files (which may contain personal or health information) may be reviewed during independent reviews of the Audit Office. Where work of the Audit Office is reviewed by a third party, that third party is bound by the same privacy principles as the Audit Office.	• request an amendment, if you believe that personal or health information held by the Audit Office is inaccurate, irrelevant, not up to date, incomplete and/or misleading, The Privacy Officer will facilitate access to and amendment of personal and health information where necessary. Individual staff members can access their employment records. <u>Accuracy</u> The Audit Office often relies on the person providing the information to confirm its accuracy and completeness. During the online recruitment application process, the applicants create a profile which they can access and update at any time. At the end of the application, a link to this Plan is included and the applicants have to declare that, to the best of their knowledge, the information provided in the application is true and correct. During onboarding or other times that health information may be disclosed for the purpose of making reasonable workplace adjustments, the information is collected from the employee. Where practical, the Audit Office will confirm personal and health information is accurate before using it. For example, staff are reminded annually to check and update their contact details within the People & Culture system. Staff with concerns about the accuracy of their personal information can discuss their concerns with People and Culture or the Privacy Officer. <u>Use</u> The Audit Office uses personal and health information for the purpose it was collected. Use of personal information is restricted to authorised staff. The Audit Office's Records Management Policy sets appropriate levels of access to all files, including those containing personal information. The contact details of staff members and their nominated emergency contacts may be used by authorised staff in case of emergency, for legitimate business purposes, e.g. providing address details to a courier. People managers have access to relevant information about their staff for review and management purposes, and to assist in the implementation of reasonable workplace adjustments.

Requirement on the AO	Audit function	Corporate function
used for the purpose it was collected or for a **directly related purpose** which a person would expect.		

7.5 Disclosure

Requirement on the AO	Audit function	Corporate function
IPP 11 and IPP 12 Sections 18 and 19 of the PPIP Act – information (including sensitive information) can only be **disclosed with consent**. **HPP 11** Schedule 1 of the HRIP Act – only disclose health information for the purpose for which it was collected, or for a directly related purpose, unless consent is given.	The Audit Office is prevented by the secrecy provisions of section 38(1) of the GSA Act and section 425(1) of the LG Act from disclosing any information (including sensitive personal information) collected during the audit process. Sections 38(2) of the GSA Act and 425(2) of the LG Act contain exceptions to the requirements of the secrecy provisions, for example the secrecy provisions do not apply where disciplinary proceedings are taken against a public official. Generally, audit teams should not include personal information in audit products provided to audited entities, even if these are not intended for publication. Personal information should not be included in any of the Audit Office's published reports. There are some limited situations where the Audit Office may be required to disclose information collected during an audit, which may include personal information. For example, the Audit Office is required to report possible corrupt conduct to the Independent Commission Against Corruption and the ICAC can issue a notice under sections 21 to 23 of the ICAC Act requiring that the Audit Office provides information. Other situations may arise where the Audit Office is legally required to disclose personal information. In addition to the secrecy requirements of the GSA Act and LG Act, the Accounting Professional and Ethical Standards Board's (APESB) APES 110 Code of Ethics for Professional Accountants	The Audit Office takes steps not to disclose sensitive personal information or health information without consent. For example, information about ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership; or information about an employee's physical or mental health As prescribed by sections 18 and 19 of the PPIP Act, there are some limited situations where the Audit Office may be required to disclose personal information, such as to deal with a serious or imminent threat to any person's health and safety. The Audit Office's Social Media Policy requires staff to: • comply with privacy legislation when using social media in personal or official capacity; and • not compromise the privacy of an individual. Public interest disclosures As an integrity agency, the Audit Office receives public interest disclosures (PIDs) from public officials reporting wrongdoing. These reports can contain personal information. The Audit Office complies with section 64 of the PID Act, which prevents the disclosure of identifying information about a reporter without their consent or in limited other circumstances. The Audit Office also has a Memorandum of Understanding with the NSW Ombudsman and a Memorandum of Understanding with the

Requirement on the AO	Audit function	Corporate function
	(including Independence Standards) (November 2018) imposes an ethical requirement on professional accountants to respect the confidentiality of information acquired as a result of professional and business relationships, not to disclose any such information to third parties without proper and specific authority, unless there is a legal or professional right or duty to disclose and not to use the information for the personal advantage of the APESB member or third parties.	Office of Local Government to cover the referral and sharing of PID information and, and complaints from members of the public. Both memoranda provide for confidentiality only allow for the sharing of personal information without consent of the reporter/ complainant in certain circumstances, i.e., when 'reasonably necessary' to assist the other agency in carrying out its functions *and* consistent with any other permissions under relevant legislative frameworks. The memoranda also state that express consent is required for the sharing of "sensitive" personal information, defined as information about ethnic or racial origin, political opinions, religious or philosophical beliefs, health, and sexual activities. The principles and approaches in these memoranda are applied by the Audit Office to referrals to other integrity agencies such as the ICAC, insofar as they are also consistent with referral requirement under the *Independent Commission Against Corruption Act 1988*.

See Appendix 1 for information regarding the Audit Office's management of health information in line with HPP12 to HPP 15.

8. Breaches of the PPIP Act and the HRIP Act

All Audit Office staff are responsible for ensuring their awareness of and compliance with privacy policies and procedures. Breach of the Audit Office's privacy policies may result in disciplinary action. Any suspected breach of privacy or a misuse of personal information must be immediately reported to the Privacy Officer or appropriate people manager. Public sector employees may be fined or imprisoned for misusing personal information under the PPIP Act and the HRIP Act.

Appendix 1 contains a list of offences under the PPIP Act and the HRIP Act.

8.1 Data Breach Management Policy

The Audit Office has a Data Breach Management Policy and accompanying procedures to provide guidance to staff on managing data breaches, including those involving personal information and those where mandatory notifications are required.

The Audit Office has an internal register to capture and report on data breaches and respond to those incidents, including 'eligible data breaches' as required under the PPIP Act.

The Audit Office also publishes the Data Breach Management Policy and public notifications register on our website.

9. Review rights and complaints

9.1 Complaints

If an individual has a complaint about how the Audit Office has dealt with their personal and health information, they can seek to resolve the matter informally by contacting the Privacy Officer with the details of the complaint. Information about how to make a complaint about the Audit Office and a copy of the Complaints Management Policy are available on the Audit Office website.

9.2 Internal review

If a person feels aggrieved by the conduct of the Audit Office in respect of a privacy issue, they are entitled to an internal review under the PPIP Act. An application for internal review must:

- be in writing
- be addressed to the Audit Office of New South Wales
- include a return address for correspondence
- be lodged within six months of the date the applicant first became aware of the conduct.

An internal review can be requested by filling out the internal review form available on the Information and Privacy Commission New South Wales (IPC) website. It is not compulsory to complete the form, however an internal review must be requested in writing.

The review will be conducted by an Officer being either:

- the Privacy Officer, or
- another member of staff appointed by the Auditor-General of New South Wales if the matter is about the conduct of the Privacy Officer.

When carrying out an internal review, the Audit Office will refer to the NSW Privacy Commissioner's (Privacy Commissioner) materials available on the IPC website, in particular the privacy internal review checklist and guidance how to handle an internal review. The Officer conducting the internal review will acknowledge receipt of a request for an internal review within seven days and complete the internal review within 60 days. The Officer will keep the applicant up to date with the progress of the internal review and will advise as soon as practicable if the review is likely to take more than 60 days.

Within 14 days of completing the review, the Officer will notify the applicant in writing about the findings of the review, the actions the Audit Office proposes to take and the right to further review.

As required by the PPIP Act, the Audit Office will:

- notify the Privacy Commissioner of an application for internal review
- keep the Privacy Commissioner informed of the progress of the review
- inform the Privacy Commissioner of the findings of the review and the action proposed to be taken in relation to the matter.

The Privacy Commissioner can make submissions to the Audit Office in relation to the subject matter of the application for internal review.

9.3 External review by the NSW Civil and Administrative Tribunal (NCAT)

If the Audit Office has not completed the review within 60 days, the applicant disagrees with the findings of the internal review or is not satisfied with the action taken by the Audit Office in relation to the application, the applicant has the right to apply to the NCAT for an external review of the conduct.

Further information about making an application to the NCAT, including the contact details can be found on the NCAT website.

9.4 Complaints to the Privacy Commissioner

An individual can make a complaint to the Privacy Commissioner about a breach of their privacy by the Audit Office. More information about the role of the IPC in handling complaints, including the contact details, can be found on the IPC website.

10. Contacting the Audit Office

For more information about this Plan or about the personal information the Audit Office holds, please contact the Privacy Officer:

Email: governance@audit.nsw.gov.au
Phone: 02 9275 7100
Post: GPO Box 12, Sydney NSW 2001

11. Review

The Plan will be reviewed at least every two years in the absence of any significant changes or more frequently where required taking into account legislative or organisational changes, risk factors and consistency with other policies. The next review is due in March 2026.

Document information

Title:	Privacy Management Plan
Owner:	Governance
Person responsible:	Executive Director, Professional Services
Last updated:	27 March 2024
Next review date:	March 2026

Document history

Version	Date	Reason for Amendment
1.0	July 2014	Privacy Management Plan document developed.
1.1	March 2015	Annual review and update.
1.2	May 2016	Annual review and update.
1.3	January 2018	Biannual review and update.
1.4	February 2018	Minor amendments made following an assessment of the Plan against the IPC Checklist for review of Privacy Management Plans.
2.0	March 2020	Biannual review and update, including formatting change.
2.1	March 2020	Minor amendments made following receipt of feedback from the IPC.
2.2	August 2022	Review and updated as per the requirement in section 33(5) of the *Privacy and Personal Information Protection Act 1998*.
2.3	February 2024	Review and updated to include content and formatting amendments, and to comply with requirements of the NSW Mandatory Notification of Data Breach Scheme and other relevant legislative amendments.

Appendix 1 – About NSW's privacy laws

This section contains a general summary of how the Audit Office must manage personal and health information under the PPIP Act, the HRIP Act and other relevant laws. For more information, please refer directly to the relevant law, contact the Audit Office or visit the Audit Office website.

1. The PPIP Act and personal information

The PPIP Act sets out how the Audit Office must manage personal information.

1.1 About personal information

Personal information is defined in section 4 of the PPIP Act and means information or an opinion about an individual whose identity is apparent or can reasonably be ascertained.

Personal information can include a person's name and address, details about their family life, their sexual preferences, financial information, fingerprints and photos. There are some kinds of information that are not personal information, such as information about someone who has been dead for more than 30 years, information about someone that is contained in a publicly available publication, or information or an opinion about a person's suitability for employment as a public-sector official. Health information is generally excluded here as it is covered by the HRIP Act.

1.2 Information protection principles (IPPs)

Part 2, division 1 of the PPIP Act contains 12 IPPs with which the Audit Office must comply. Below is an overview of the principles as they apply to the Audit Office.

Collection

1. The Audit Office collects personal information only for a lawful purpose that is directly related to the Audit Office's functions and activities.
2. In the exercise of its corporate functions, the Audit Office collects personal information directly from the person concerned.
3. The Audit Office informs people why their personal information is being collected, what it will be used for, and to whom it will be disclosed. The Audit Office will tell people how they can access and amend their personal information and any possible consequences if they decide not to give their personal information to the Audit Office.
4. The Audit Office ensures personal information is relevant, accurate, not excessive and does not unreasonably intrude into the personal affairs of people.

Storage

5. The Audit Office stores personal information securely, keeps it no longer than necessary and destroys it appropriately. Personal information is protected from unauthorised access, use, or disclosure.

Access and accuracy

6. The Audit Office is transparent about any personal information stored, what it is used for and the right to access and amend it.
7. The Audit Office allows people to access their own personal information without unreasonable delay or expense.
8. The Audit Office allows people to update, correct, or amend their personal information where necessary.
9. The Audit Office makes sure that personal information is relevant and accurate before using it.

Use

10. The Audit Office only uses personal information for the purpose it was collected for unless the person consents to the information being used for an unrelated purpose.

Disclosure

11. The Audit Office will only disclose personal information with people's consent unless they were already informed of the disclosure when the personal information was collected.
12. The Audit Office does not disclose, without consent, sensitive personal information, such as ethnicity or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities, or trade union membership.

1.3 Exemptions to the IPPs

Part 2, division 3 of the PPIP Act contains exemptions that may allow the Audit Office to not comply with IPPs in certain situations.

The Audit Office is not required to comply with IPPs with respect to the collection, use or disclosure of personal information if the collection, use or disclosure of the information is reasonably necessary to enable the auditing of the accounts or performance of a public-sector agency or group of public sector agencies.

Public interest directions can modify the IPPs for any NSW public sector agency. These are available on the IPC website. Currently, there are none that are likely to affect how the Audit Office manages personal information.

1.4 Offences

Offences can be found in part 8 of the PPIP Act. It is an offence for the Audit Office to:

- intentionally disclose or use personal information about an individual to which the official has or had access to in the exercise of his or her official functions
- offer to supply personal information that has been disclosed unlawfully
- hinder the Privacy Commissioner or a staff member from doing their job.

1.5 Public registers

Part 6 of the PPIP Act also governs how NSW public sector agencies should manage personal information contained in public registers. The Audit Office maintains the following public registers that can include personal information:

- Conflict of interest registers - Audit and Risk Committee, Office Executive, and Renumerations Committee
- Act of Grace payment registers
- Gifts of Government property registers

At the time of publishing this Policy, only the conflict of interest registers contain personal information. Other registers are blank. The personal information contained in the conflict of interest registers is consistent with the requirements of the PPIP Act because the information relates to the purpose of the register.

The PPIP Act states that the public notifications register of mandatory data breaches, published under section 59P of the PPIP Act, should not include personal information.

Individuals who have personal information contained in a public register can contact the Audit Office Governance team with inquiries about accessing or applying for a suppression of personal or health information in a public register.

2. The HRIP Act and health information

The HRIP Act sets out how the Audit Office must manage health information.

2.1 About health information

Health information is a more specific type of personal information and is defined in section 6 of the HRIP Act. Health information can include information about a person's physical or mental health, such as a psychological report, blood test, an X-ray, or even information about a person's medical appointment. It can also include personal information that is collected to provide to a health service, such as a name and contact number on a medical record.

2.2 Health privacy principles (HPPs)

Schedule 1 of the HRIP Act contains 15 HPPs that the Audit Office must comply with. Below is an overview of the principles as they apply to the Audit Office.

Collection

1. The Audit Office collects health information only for lawful purposes that are directly related to the Audit Office's functions and activities.
2. The Audit Office makes sure health information is relevant, accurate, not excessive and does not unreasonably intrude into the personal affairs of people.
3. In the exercise of its corporate functions, the Audit Office collects health information directly from the person concerned (where possible).
4. The Audit Office informs people why their health information is being collected, what it will be used for and to whom it will be disclosed. The Audit Office will tell people how they can access and amend their health information and any possible consequences if they decide not to give their health information to the Audit Office.

Storage

5. The Audit Office stores health information securely, keeps it no longer than necessary and destroys it appropriately. Health information is protected from unauthorised access, use, or disclosure.

Access and accuracy

6. The Audit Office is transparent about the health information stored about people, what the information is used for and the right to access and amend it.
7. The Audit Office allows people to access their own health information without unreasonable delay or expense.
8. The Audit Office allows people to update, correct, or amend their health information where necessary.
9. The Audit Office makes sure the health information is relevant and accurate before using it.

Use

10. The Audit Office only uses health information for the purpose it was collected for, unless the person consents to the information being used for an unrelated purpose.

Disclosure

11. The Audit Office will only disclose health information with people's consent, unless they were already informed of the disclosure when the health information was collected.

Identifiers and anonymity

12. The Audit Office does not use unique identifiers for health information, as they are not needed to carry out the functions of the Audit Office. Information for audit teams specifies that audit teams should remove unique identifiers from health information that is received.
13. The Audit Office allows people to stay anonymous where it is lawful and practical.

Transfers and linkage

14. The Audit Office does not usually transfer health information outside of NSW.
15. The Audit Office does not currently use a health records linkage system and does not anticipate using one in the future. However, if one were to be used, the Audit Office would not use one without people's consent.

2.3 Exemptions to the HPPs

Clause 10(b) schedule 1 to the HRIP Act permits an agency to use health information for a secondary purpose if:

- the secondary purpose is directly related to the primary purpose and
- it can be reasonably expected the agency will use the information for the secondary purpose.

The IPC statutory guidelines on the management of health services clarifies that the 'direct relation exemption' in clause 10(b) schedule 1 to the HRIP Act includes 'some quality assurance activities carried out by the organisation such as monitoring, evaluating, auditing the provision of the particular product or service the organisation has or is providing the person'.

Health privacy codes of practice and public interest directions can modify the HPPs for any NSW public sector agency. These are available on the IPC website. Currently, there are none that are likely to affect how the Audit Office manages health information.

2.4 Offences

Offences can be found in part 8 of the HRIP Act. It is an offence for the Audit Office to:

- intentionally disclose or use health information about an individual to which the official has or had access to in the exercise of his or her official functions
- offer to supply health information that has been disclosed unlawfully
- attempt to persuade an individual to refrain from making or to withdraw an application pursuing a request for access to health information or a complaint to the Privacy Commissioner or NCAT
- by threat, intimidation, or false representation require another person to give consent or to do, without consent, an act for which consent is required.

Appendix 2: Other applicable laws

This section contains information about the other laws that affect how the Audit Office complies with the IPPs and HPPs.

2.1 GSA Act

Section 38(1) of the GSA Act provides that the Audit Office must preserve and aid secrecy with respect to all matters and things that come to our knowledge in undertaking functions under the GSA Act, such as information collected during the audit process.

Section 38(2) contains exceptions to the requirements of the secrecy provisions, for example the secrecy provisions do not apply where disciplinary proceedings are taken against a public official.

2.2 LG Act

Section 425(1) of the LG Act provides that the Audit Office must preserve and aid secrecy with respect to all matters and things that come to our knowledge in undertaking functions under the LG Act, such as information collected during the audit process.

Section 425(2) contains exceptions to the requirements of the secrecy provisions, for example the secrecy provisions do not apply where disciplinary proceedings are taken against a public official.

2.3 Crimes Act

Under part 6 of the Crimes Act, the Audit Office must not access or interfere with data in computers or other electronic devices unless it is authorised to do so.

2.4 GIPA Act and GIPA Regulation

The object in the GIPA Act is to maintain and advance a system of responsible and representative democratic government that is open, accountable, fair and effective by providing access to government information. To support this, the GIPA Act focuses on making government information more readily available to the public. This means the Audit Office must release information unless there is an overriding public interest against doing so.

The GIPA Act provides a mechanism to access personal information or other information. An application can be made to the Audit Office to access information that the Audit Office holds. Sometimes, this information may include personal and/or health information.

The GIPA Act lists a number of considerations which can be taken into account when deciding not to release information to the public. These considerations include whether the disclosure would:

- reveal an individual's personal information
- contravene IPPs under the PPIP Act or the HPPs under the HRIP Act.

In addition, the GIPA Act contains specific provisions relating to information collected during the audit process. Schedule 2 of the GIPA Act provides that the information 'related to' the investigative, audit and reporting functions of the Audit Office is classified as excluded information. When information is classified as excluded information it is presumed that there is an overriding public interest against disclosing that information.

In practice, this means that any information (including personal information) that the Audit Office has collected during its investigating, auditing or reporting functions will not be disclosed by the Audit Office in response to a GIPA request.

2.5 ICAC Act

Under section 8(1)(d) of the ICAC Act, the Audit Office staff cannot misuse information acquired in the course of their official functions.

The Audit Office has an obligation under section 11 of the ICAC Act to report suspected corrupt conduct to the ICAC. In fulfilling this obligation, the Audit Office may be required to disclose information collected during an audit.

2.6 PID Act

The PID Act sets in place a system to encourage public officials to report serious wrongdoings. The Audit Office can receive and 'deal with PIDs about the serious and substantial waste of public money. The Audit office must also appropriately deal with PID about serious wrongdoing that relate to the Audit Office, including by referring these to another relevant integrity agency. The definition of personal information under the PPIP Act excludes information contained in a PID. This means that personal information received or collected under the PID Act is not subject to the IPPs or HPPs.

The PID Act (section 64) requires the Audit Office does not disclose information tending to identify a person as the maker of a voluntary PID, with exceptions such as if the person consents to this in writing or if it is considered reasonably necessary to protect the person from detriment. This Plan includes information on how the Audit Office's protects information received in relation to PIDs. For further information, refer to the Audit Office's Internal Public Interest Disclosure Policy, and External Public Interest Disclosure Policy.

Memorandum of Understanding between other integrity agencies sets out how information is to be handled when referring complaints and PIDs to other agencies.

2.7 State Records Act and State Records Regulation

Defines the circumstances under which the Audit Office can destroy its records. It also authorises the State Archives and Records Authority to establish policies, standards and codes to ensure that NSW public sector agencies manage their records appropriately.

Appendix 3: Audit Office privacy-related policies

Title	Issue covered	Author	Access
Code of Conduct	Maintaining confidentiality and protecting personal information and privacy.	Audit Office	Website
Statement of Business Ethics	Maintaining confidentiality.	Audit Office	Website
Complaints Management Policy	Maintaining confidentiality and managing personal information in accordance with the IPPs in the PPIP Act.	Audit Office	Website
Conflict of Interest Policy and Professional Independence Policy	Maintaining confidentiality and managing personal information in accordance with the IPPs in the PPIP Act.	Audit Office	Website
Internal Public Interest Disclosures Policy **and** External Public Interest Disclosures Policy	Maintaining confidentiality of the reporter.	Audit Office	Website
Fraud and Corruption Control Policy	Maintaining confidentiality.	Audit Office	Website
Respectful Workplace Policy	Maintaining confidentiality.	Audit Office	Website
Social Media Policy	Maintaining confidentiality and protecting privacy of individuals.	Audit Office	Website
Third Party Security Policy	Formal agreements with third parties to comply with the PPIP Act and *Privacy Act 1988*.	Audit Office	Website
Data Breach Management Policy	Managing data breaches.	Audit Office	Website
Office Executive Charter	Maintaining confidentiality.	Audit Office	Website
Audit and Risk Committee Charter	Maintaining confidentiality.	Audit Office	Website
Remuneration Committee Charter	Maintaining confidentiality.	Audit Office	Website
Internal Audit Charter	Maintaining confidentiality.	Audit Office	Website
Website Privacy Policy	Managing personal information in accordance with the IPPs in the PPIP Act.	Audit Office	Website
Records Management Policy	Ensuring that personal information is stored, retained and disposed of appropriately.	Audit Office	Intranet
Secure Desk and Documentation Policy	Ensuring that personal information is stored, retained and disposed of appropriately.	Audit Office	Intranet
Office Access Policy	Ensuring that personal information is stored, retained and disposed of appropriately.	Audit Office	Intranet
Internal Audit Manual	Maintaining confidentiality.	Audit Office	Intranet
ICT Acceptable Use Policy	Maintaining confidentiality and protecting personal information and privacy.	Audit Office	Intranet

Title	Issue covered	Author	Access
Bring Your Own Device (BYOD) Policy	Guidance for the secure use and the data contained on the devices.	Audit Office	Intranet
Mobile Device and Remote Working Policy	Maintaining confidentiality and protecting personal information and privacy.	Audit Office	Intranet
Information Security Policy	Maintaining confidentiality and protecting personal information and privacy.	Audit Office	Intranet
Physical Security Policy	Details the requirements for the implementation of physical security controls around the Audit Office's facilities.	Audit Office	Intranet
Workplace Surveillance Policy	Protecting personal information and privacy.	Audit Office	Intranet
ISMS Framework	Maintaining confidentiality.	Audit Office	Intranet
Grievance Policy	Maintaining confidentiality and protecting personal information and privacy.	Audit Office	Intranet