audit office
OF NEW SOUTH WALES

Privacy Management Plan

March 2020

INSIGHTS FOR BETTER GOVERNMENT

contents

1.	**Introduction**	**1**
2.	**About the Audit Office**	**1**
3.	**Legislative framework**	**1**
4.	**Policy and procedure development**	**2**
5.	**Promoting the Plan**	**2**
5.1	Audit Office staff	2
5.2	Public awareness	2
6.	**The Privacy Contact Officer**	**3**
7.	**How the Audit Office manages personal and health information**	**3**
7.1	Functions of the Audit Office	3
7.2	Collection	4
7.3	Storage	7
7.4	Access and accuracy	8
7.5	Use	9
7.6	Disclosure	10
8.	**Breaches of the Privacy Act and the Health Records Act**	**11**
8.1	Data Breach Management Policy	11
9.	**Review rights and complaints**	**11**
9.1	Complaints	11
9.2	Internal review	11
9.3	External review by the NSW Civil and Administrative Tribunal	12
9.4	Complaints to the Privacy Commissioner	12
10.	**Contacting the Audit Office**	**12**
11.	**Review**	**12**
Appendix 1: About NSW's privacy laws		**13**
1.	**The Privacy Act and personal information**	**13**
1.1	About personal information	13
1.2	Information protection principles (IPPs)	13
1.3	Exemptions to the IPPs	14
1.4	Offences	14
1.5	Public registers	14
2.	**The Health Records Act and health information**	**14**
2.1	About health information	14
2.2	Health privacy principles (HPPs)	14
2.3	Exemptions to the HPPs	16

2.4 Offences 16
Appendix 2: Other applicable laws 17
2.1 Government Sector Audit Act 17
2.2 Local Government Act 17
2.3 Crimes Act 17
2.4 GIPA Act and GIPA Regulation 17
2.5 ICAC Act 17
2.6 PID Act 18
2.7 State Records Act and State Records Regulation 18
Appendix 3: Audit Office privacy-related policies 19

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* (the Privacy Act) to have 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 Privacy Act.

2. About the Audit Office

The Audit Office is a statutory authority, established under the *Government Sector Audit Act 1983* (the Government Sector Audit 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 Government Sector Audit Act and the *Local Government Act 1993* (Local Government 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 Privacy 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 Privacy Act contains 12 Information Protection Principles (IPPs) which cover the key areas of:

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

In addition to the Privacy Act, the *Health Records and Information Privacy Act 2002* (the Health Records 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:

- *Privacy and Personal Information Protection Regulation 2019*
- *Health Records and Information Privacy Regulation 2017*
- Government Sector Audit Act
- Local Government Act
- *Crimes Act 1900* (the Crimes Act)
- *Government Information (Public Access) Act 2009* (GIPA Act)
- *Government Information (Public Access) Regulation 2009* (GIPA Regulation)
- *Independent Commission Against Corruption Act 1988* (ICAC Act)
- *Public Interest Disclosures Act 1994* (PID Act)
- *State Records Act 1998* (State Records Act) and
- *State Records Regulation 2015* (State Records Regulation)

[1] References to personal information include health information unless otherwise specified.

Appendix 2 contains additional information about these Acts and Regulations.

4. Policy and procedure development

To ensure compliance with the requirements of section 33(2) of the Privacy Act, the Audit Office is required to set out in this Plan how policies and practices are developed. This Plan sets out a number of specific elements of the Audit Office's privacy protection framework. Policies and practices 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
- 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 and health information is managed, the Audit Office consults with the applicable parties to ensure compliance with the Privacy Act and the Health Records Act.

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

5. Promoting the Plan

The Audit Office reinforces transparency and compliance with the Privacy Act and the Health Records Act by:

- endorsing the Plan and making it publicly available
- ensuring the Plan is regularly reviewed and updated as appropriate
- reporting on privacy issues in the Audit Office annual report in accordance with the provisions of the *Annual Reports (Statutory Bodies) Act 1985*
- undertaking a biennial self-assessment of compliance with the Privacy Act
- confirming support for privacy compliance in the 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 Contact Officer (the Executive Manager 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 and health 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 and health information.

6. The Privacy Contact Officer

The Privacy Contact 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 Privacy Act and the Health Records Act.

The Privacy Contact Officer is the first point of contact 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 and health information

7.1 Functions of the Audit Office

7.1.1 Audit function

The Audit Office may receive personal 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 Privacy 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.

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 Privacy Act and the HPPs of the Health Records Act.

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 Privacy Act and the Health Records Act in the way it manages personal and health information obtained as part of the corporate functions.

7.2 Collection

Legislation	Audit function	Corporate function
IPP 1 Section 8 of the Privacy 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 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) – 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.

Legislation	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. The Audit Office has a specific function under the PID Act to receive public interest disclosures (PIDs) about serious and substantial waste in NSW Government agencies, universities and local councils. The Audit Office complies with section 22 of the PID Act with regards to maintaining the confidentiality of the person making a PID. In addition, the Audit Office receives complaints and feedback from members of the public about the entities the Audit Office audits, and occasionally about the office itself. These PIDs, complaints and feedback usually contain 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. Section 4(5) of the Privacy Act provides that personal information 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 on 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 receives information from other oversight agencies, 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 oversight agencies. 14. The Audit Office collects health information about staff including: – medical certificates – health declarations showing medical conditions – fitness for duty assessments[2]

[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 office and also receives a copy. The information in the report is treated in accordance with the Privacy Act and the Health Records Act.

Legislation	Audit function	Corporate function
		– workers compensation records – workplace health and safety records – other medical information.
IPP 2 Section 9 of the Privacy Act – information must be collected **directly** from the individual.	Any personal or health information collected during an audit is collected from the agency being audited – see section 27A(b)(iii) of the Privacy Act.	In most circumstances personal information is collected directly from employees. For example, information in the online recruitment application and in the onboarding form. 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 Privacy Act – a public sector agency must 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.
IPP 4 Section 11 of the Privacy Act – a public sector agency must take reasonable steps to ensure the information collected is **relevant**, **not excessive**, **accurate**, **up to date** and **complete**.	The Audit Office only collects personal information to support the conduct of financial and performance audits.	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 update their personal information using online systems.

7.3 Storage

Legislation	Audit function and corporate function
IPP 5 Section 12 of the Privacy Act – information must be **stored securely**, **kept no longer than necessary** and **destroyed appropriately**.	The Audit Office has a number of policies in place (available on the intranet) to ensure that personal 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 information are retained in accordance with the retention and disposal authorities made under the State Records Act. Most of the personal information collected or held by the Audit Office is stored electronically. 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 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.

Legislation	Audit function	Corporate function
IPP 5 Section 12 of the Privacy Act – information must be **protected** from unauthorised access, use, or disclosure.	Personal 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 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 Audit Office ISMS Framework. Staff access to the network is restricted by an individual user ID and password. The Audit Office Secure Desk and Documentation Policy provides for 'a clean desk' approach, which means 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 and accuracy

Legislation	Audit function	Corporate function
IPP 6 Section 13 of the Privacy Act – a public sector agency must **enable** the individual to **find out if the agency holds the information** relating to the individual. **IPP 7 and IPP 8** Sections 14 and 15 of the Privacy Act – a public sector agency must allow: • **access** to personal information **without**	The Audit Office does not collect personal 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 information which has been obtained by the Audit Office as part of an audit should contact the agency providing the information.	Everyone has the right to access and amend the personal and/or 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/or 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 and/or health information. Contact the Privacy Contact Officer (Executive Manager, Governance (Legal)) to: • find out whether the Audit Office holds personal information about you • make an access request, or • request an amendment, if you believe that personal information held by the Audit Office is inaccurate, irrelevant, not up to date, incomplete and/or misleading,

Legislation	Audit function	Corporate function
excessive delay or expense • **update, correction, or amendment** of personal information.		The Privacy Contact Officer will facilitate access to and amendment of personal information where necessary. Individual staff members can access their employment records, and people managers have access to defined information about their staff for review and management purposes.
IPP 9 Section 16 of the Privacy Act – the personal information must be **relevant**, **accurate**, **up to date** and **complete**.	The Audit Office relies on the agency providing the information to confirm its accuracy, currency, and completeness.	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. Whenever possible, the Audit Office will ensure personal information is accurate before using it. For example, staff are reminded annually to check and update their contact details within the HR system. Staff with concerns about the accuracy of their personal information can discuss their concerns with Human Resources or the Privacy Contact Officer.

7.5 Use

Legislation	Audit function	Corporate function
IPP 10 Section 17 of the Privacy Act – the personal information must be **used for a purpose it was collected**.	Personal information collected during the audit process is only used for the purpose of the audit. The audit files (which may contain personal 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.	The Audit Office uses personal information for the purpose it was collected. Use of personal information is restricted to authorised staff. The Audit Office 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.

7.6 Disclosure

Legislation	Audit function	Corporate function
IPP 11 and IPP 12 Sections 18 and 19 of the Privacy Act – information (including sensitive information) can only be **disclosed with consent**.	The Audit Office is prevented by the secrecy provisions of section 38(1) of the Government Sector Audit Act and section 425(1) of the Local Government Act from disclosing any information (including sensitive personal information) collected during the audit process. Sections 38(2) of the Government Sector Audit Act and 425(2) of the Local Government 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. There are some limited situations where the Audit Office may be required to disclose information collected during an audit. For example, the Audit Office is required to report possible corrupt conduct to the Independent Commission Against Corruption. Other situations may arise where the Audit Office is legally required to disclose personal information. In addition to the secrecy requirements of the Government Sector Audit Act and Local Government Act, the Accounting Professional and Ethical Standards Board's (APESB) Code of Ethics for Professional Accountants (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.	The Audit Office will not disclose personal information unless permitted by sections 18 and 19 of the Privacy Act. The Audit Office will take particular care not to disclose sensitive personal information without consent. For example, information about ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership. The Audit Office will only disclose sensitive information without consent in order 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 connection with their employment; and • not compromise the privacy of an individual. As part of the oversight agency role, the Audit Office has a Memorandum of Understanding with the NSW Ombudsman and a Memorandum of Understanding with the Office of Local Government to cover the referral and sharing of information about PIDs and complaints. Both memoranda provide for confidentiality of information shared.

8. Breaches of the Privacy Act and the Health Records 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 Contact Officer or appropriate people manager. Public sector employees may be fined or imprisoned for misusing personal information under the Privacy Act and the Health Records Act.

Appendix 1 contains a list of offences under the Privacy Act and the Health Records Act.

8.1 Data Breach Management Policy

The Audit Office has a Data Breach Management Policy to provide guidance to staff on managing data breaches, including those involving personal information. The Audit Office also has a register to capture and report on data breach incidents and response to those incidents.

9. Review rights and complaints

9.1 Complaints

If an individual has a complaint about how the Audit Office has dealt with their personal information, they can seek to resolve the matter informally by contacting the Privacy Contact 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 Privacy 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 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 the Privacy Contact Officer or another member of staff appointed by the Auditor-General if the matter is about the conduct of the Privacy Contact Officer.

When carrying out an internal review, the Audit Office will refer to the Privacy Commissioner's guidance materials available on the IPC website, in particular the Privacy Internal Review Checklist and guidance for conducting internal reviews.

The Audit Office will acknowledge receipt of a request for an internal review within seven days and complete the internal review within 60 days. The Privacy Contact 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 Audit Office 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 Privacy 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.

Pursuant to clause 10 of the *Annual Reports (Statutory Bodies) Regulation 2015*, the Audit Office will record requests for and outcomes of any internal reviews conducted in its annual report.

9.3 External review by the NSW Civil and Administrative Tribunal

If the Audit Office has not completed the review within 60 days or 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 NSW Civil and Administrative Tribunal for an external review of the conduct.

Further information about making an application to the tribunal can be found on their website. The contact details for the tribunal are:

Phone: 1300 006 228
Address: Level 10, John Maddison Tower, 86-90 Goulburn Street, Sydney NSW 2000

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 can be found on the IPC website. The contact details for the IPC are:

Email: ipcinfo@ipc.nsw.gov.au
Phone: 1800 472 679
Post: GPO Box 7011, Sydney NSW 2001

10. Contacting the Audit Office

For more information about this Plan or about the personal information the Audit Office holds, please contact the Privacy Contact 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 2022.

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 Privacy Act, the Health Records 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 Privacy Act and personal information

The Privacy 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 Privacy Act and is essentially any information or opinions about a person where that person's identity is apparent or can be reasonably 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 Health Records Act.

1.2 Information protection principles (IPPs)

Part 2, Division 1 of the Privacy 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 Privacy 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 Privacy 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 Privacy Act also governs how NSW public sector agencies should manage personal information contained in public registers. The Audit Office neither holds nor maintains any public registers, so this section of the Privacy Act does not apply to the Audit Office.

2. The Health Records Act and health information

The Health Records 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 Health Records 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 Health Records 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.

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 Health Records 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 Health Records 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 Health Records 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 Tribunal
- 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 Government Sector Audit Act

Section 38(1) of the Government Sector Audit Act provides that the Audit Office must preserve and aid secrecy with respect to all matters and things that are part of the 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 Local Government Act

Section 425(1) of the Local Government Act provides that the Audit Office must preserve and aid secrecy with respect to all matters and things that are part of the 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 Privacy Act or the HPPs under the Health Records 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 collected as part of 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 wrongdoings. The Audit Office is responsible for receiving complaints made as PIDs about serious and substantial waste, as provided under the PID Act. The definition of personal information under the Privacy 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 requires the Audit Office to not disclose information that might identify or tend to identify a person who has made a PID. This Plan includes the Audit Office's procedures to protect the information received in relation to PIDs. For further information, refer to the Audit Office's Internal and External Public Interest Disclosures Policies.

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 Privacy 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
Website Privacy Policy	Managing personal information in accordance with the IPPs in the Privacy Act.	Audit Office	Website
Social Media Policy	Maintaining confidentiality and protecting privacy of individuals.	Audit Office	Website
Internal Public Interest Disclosures Policy **and** External Public Interest Disclosures Policy	Maintaining confidentiality of the reporter.	Audit Office	Website
Conflict of Interest Policy and Professional Independence Policy	Maintaining confidentiality and managing personal information in accordance with the IPPs in the Privacy Act.	Audit Office	Website
Internal Audit Manual	Maintaining confidentiality.	Audit Office	Intranet
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
Data Breach Management Policy	Managing data breaches.	Audit Office	Intranet
ICT Acceptable Use Policy	Maintaining confidentiality and protecting personal information and privacy.	Audit Office	Intranet
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

Title	Issue covered	Author	Access
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