



Audit Office of New South Wales

Privacy Management Plan

May 2016

Table of Contents

Table of Contents	2
1 Introduction	3
2 About the Audit Office of New South Wales	3
3 Legislative framework	3
4 How the Audit Office manages personal and health information	3
4.1 Audit function.....	3
4.1.1 Collection.....	4
4.1.2 Storage.....	4
4.1.3 Access and accuracy	4
4.1.4 Use	4
4.1.5 Disclosure.....	4
4.2 Public interest disclosures and complaints.....	5
4.3 Corporate functions	5
4.3.1 Collection.....	5
4.3.2 Storage.....	6
4.3.3 Access and accuracy	6
4.3.4 Use	7
4.3.5 Disclosure.....	7
5 How to access and amend personal and health information	7
6 Privacy management	7
6.1 The Privacy Contact Officer	7
6.2 Promoting the plan	7
7 Breaches of the Privacy Act	8
8 Review rights and complaints	8
8.1 Complaints	8
8.2 Internal review	8
8.3 External review by the NSW Civil and Administrative Tribunal	8
8.4 Complaints to the Privacy Commissioner.....	9
9 Contacting us	9
10 Documentation and version	9
11 Appendix 1: privacy and personal information – definitions	10
11.1 Privacy.....	10
11.2 Personal information	10
11.3 Health information	10
12 Appendix 2: Audit Office privacy related policies	11
13 Appendix 3: Other legislation	12
13.1 <i>Government Information (Public Access) Act 2009</i>	12
13.2 <i>Public Finance and Audit Act 1983</i>	12

1 Introduction

The Audit Office of New South Wales is required by section 33 of the *Privacy and Personal Information Protection Act 1998* (the Privacy Act) to have a Privacy Management Plan. This plan includes information on the type of personal information we hold, 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 of New South Wales

The Audit Office is a statutory authority, established under the *Public Finance and Audit Act 1983* which conducts financial and performance audits for the Auditor-General. The Auditor-General helps parliament hold government accountable for its use of public resources.

Our main clients are the Parliament of New South Wales, NSW Government agencies and the people of New South Wales. Further information about the functions of the Audit Office is contained in the *Information Guide* 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. Appendix 1 contains information on the definition of 'privacy' and 'personal information'.

The Privacy Protection Act includes 12 Information Protection Principles which cover the key areas of:

- collection
- storage
- access and accuracy
- use
- disclosure.

A summary of the Information Protection Principles in the Privacy Protection Act is located on the Information and Privacy Commission's (IPC) [website](#).

In addition to the Privacy Protection Act, there is a separate piece of legislation covering health records and information, the *Health Records and Information Privacy Act 2002* (the Health Records Act). The Health Records Act contains specific provisions about the management of health information and also contains a set of [Health Privacy Principles](#).

The vast majority of the personal information held by the Audit Office is subject to the Privacy Act. The Audit Office's Code of Conduct requires that all staff comply with the Privacy Act and Appendix 2 contains a summary of the Audit Office's privacy related policies.

In addition to the Privacy Act and the Health Records Act, the Audit Office must also comply with the provisions of the *Government Information (Public Access) Act 2009* and the *Public Finance and Audit Act 1983*. Appendix 3 contains additional information about these Acts.

4 How the Audit Office manages personal and health information

4.1 Audit function

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

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 information protection principles with respect to the collection, use or disclosure of personal information to enable the auditing of the accounts or performance of a public sector agency.

Despite this exemption the Audit Office does take steps to ensure that it complies with the intent of the legislation with regards to the collection, use and disclosure of personal information.

This exemption does not apply to health information as defined in the Health Records Act.

4.1.1 Collection

Personal information collected during the audit process may include names, contact details, payroll information, employment details and details of contractual arrangements as well as information used in our audits.

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.

Any personal or health information collected during an audit is collected from the agency being audited.

The Audit Office only collects information for lawful purposes.

4.1.2 Storage

The Audit Office has a number of policies in place to ensure that personal information is stored, retained and disposed of appropriately including:

- Records Management Policy
- Secure Desk Policy
- Office Access Policy
- Information Security Policy.

Personal information collected during an audit is stored in electronic audit files. Only authorised staff members have access to these files. All records are stored and disposed of in accordance with the *State Records Act 1998*.

4.1.3 Access and accuracy

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 personal information which has been obtained in this way should contact the agency providing the information.

4.1.4 Use

Personal information collected during the audit process is only used for the purpose of the audit. Our audit files (which may contain personal information) may be reviewed during independent reviews of our work. Where our work is reviewed by a third party, they are bound by the same privacy principles as the Audit Office.

4.1.5 Disclosure

The Audit Office is prevented by the secrecy provisions of section 38(1) of the *Public Finance and Audit Act 1983* from disclosing **any** information (including personal information) collected during the audit process. Section 38(2) does 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, we are required to report corrupt conduct to the Independent Commission against Corruption. Other situations may arise where we are legally required to disclose personal information.

In addition to the requirements of the *Public Finance and Audit Act 1983*, the Accounting Professional & Ethical Standards Board *Code of Ethics for Professional Accountants* (December 2010) imposes an ethical requirement on accounting professionals to ensure information remains confidential unless there is a legal or professional right or duty to disclose.

4.2 Public interest disclosures and complaints

The Audit Office has a specific function under the *Public Interest Disclosures Act 1994* to receive public interest disclosures about serious and substantial waste in government agencies. In addition, we receive complaints from members of the public about the agencies we audit, and occasionally about the office itself. These disclosures and complaints usually contain personal information about the person making the disclosure and may also contain personal information about a third party.

The Privacy Act provides if the personal information is unsolicited (as with public interest disclosures and complaints), then an agency is not considered to have collected the information. This means we are not required to comply with the information protection principles on collection of information.

In addition, the Audit Office ensures it complies with section 22 of the *Public Interest Disclosures Act 1994* with regards to maintaining the confidentiality of the person making a disclosure

4.3 Corporate functions

The Audit Office complies with the Privacy Act in the way it manages personal information about its staff and members of the public

4.3.1 Collection

The Audit Office collects personal information in a number of different ways:

- Recruitment and staff records including:
 - leave and payroll data
 - wage and salary entitlements
 - address details
 - emergency contact information
 - performance reviews and development plans
 - recruitment information
 - attendance and overtime records
 - training and development activities
 - use of information technology resources.
- Information about visitors and contractors – including name, contact details and employer details.
- Information collected for surveys and mailing lists – name, email, and contact details.

- Information collected as part of [Government Information \(Public Access\) Act 2009](#) requests, complaints and the correspondence management process – including name, contact details and other personal information specific to a particular matter.
- Visits to the Audit Office website (see the [Privacy Policy](#) for our website for more information).

The Audit Office collects health information about our staff including:

- medical certificates
- workers compensation information
- medical information.

Any health information we collect about our staff is managed in accordance with the Health Records Principles in the Health Records Act.

The Audit Office only collects such information as is reasonably necessary to fulfil our functions and activities.

Personal information collected during our audits is covered by section 4.1 of this plan.

4.3.2 Storage

The Audit Office complies with the [State Records Act 1998](#) when managing all personal information

The policies referred to in section 4.1.2 also govern how the Audit Office manages the storage of the personal information referred to in 4.3.1 above. Records containing personal information are retained in accordance with the retention and disposal authorities made under the *State Records Act 1998*.

Hard and soft copy information is stored securely in our office at 1 Margaret Street, Sydney, NSW, 2000 and in a secure NSW Government storage facility. Hard copy personal information about our employees is stored in locked cabinets. Access to files containing personal information about our employees is restricted to authorised staff.

Our records management system contains restrictions and controls to make sure that personal information about our staff stored electronically can only be accessed by authorised staff.

Our Information Security Policy and the [Privacy Policy](#) for our website apply to the personal information we hold electronically.

In addition, the Audit Office's Working from Home Policy provides that before staff is permitted to work from home 'the Audit Office must be satisfied that appropriate measures are in place to protect confidential material, and the privacy of clients...'

4.3.3 Access and accuracy

This plan provides general information on the personal information held by the Audit Office. Anyone wishing to find out what, if any, personal information the Audit Office holds about them should contact the Privacy Contact Officer using the details in section 9 below. The Privacy Contact Officer will facilitate access to personal information and work with individuals who are requesting an amendment to their personal information.

Individual staff members can access to their own employment records and managers also have access to defined information about their staff for review and management purposes. Guidance is available on the Audit Office intranet for staff on how to view and amend their personal information. Staff with concerns about the accuracy of their personal information can discuss their concerns with the Privacy Contact Officer.

4.3.4 Use

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. Staff access to the network is restricted by an individual user ID and password.

4.3.5 Disclosure

The Audit Office will only disclose personal information if the requirements of section 18 of the Privacy Act are met or where permitted by legislation or a public interest direction made under the Privacy Protection Act.

The Audit Office complies with section 19(1) of the Privacy Act which places special restrictions on the disclosure of sensitive personal information and section 19(2) of the Privacy Act which restricts the disclosure of personal information to jurisdictions outside New South Wales or to a Commonwealth agency.

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 to compromise the privacy of an individual.

The Audit Office does not maintain any public registers as defined in the Privacy Act.

5 How to access and amend personal and health information

To access or amend personal information contact the Privacy Contact Officer, using the details in section 9 below.

6 Privacy management

6.1 The Privacy Contact Officer

The Governance Manager, Open Government and Risk Management is the designated Privacy Contact Officer (see contact details in section 9 below) for the Audit Office and is responsible for this plan and any associated policies and procedures that help the Audit Office to meet its obligations under the Privacy 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 policies and procedures are fully implemented.

6.2 Promoting the plan

The Audit Office is committed to making our staff aware of their privacy obligations and in addition to providing a copy of this plan on our intranet site we:

- highlight the plan at least once a year during Privacy Awareness Week
- provide advice and guidance to staff when required
- report on privacy in our annual report
- provide updates to staff on changes to the legislation and key developments in the field.
- undertake an annual self assessment of our compliance with the Privacy Act and report on the results to senior management

7 Breaches of the Privacy Act

All Audit Office staff is responsible for ensuring their awareness of and compliance with privacy policies and procedures. Any breach of the Audit Office's privacy policies may result in disciplinary action. Public sector employees may be fined or imprisoned for misusing personal information under the Privacy Act.

Any suspected breach of privacy or a misuse of personal information must be immediately reported to the Privacy Contact Officer or appropriate manager.

8 Review rights and complaints

8.1 Complaints

If an individual has a complaint about how the Audit Office has dealt with their privacy, 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 and a copy of our Complaints Management Policy are available on our [website](#).

8.2 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 you first became aware of the breach.

An internal review can be requested by filling out the internal review [form](#) on the Information and Privacy Commission website. It is not compulsory to complete the form however you must request an internal review in writing.

The review will be conducted by the Privacy Contact Officer. If the matter is about the conduct of the Privacy Contact Officer, the Auditor-General will appoint another member of staff to conduct the review.

The Audit Office will acknowledge receipt of a request for an internal review within seven days. We will complete all internal reviews 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 (email, letter or fax) about the actions we propose to take and the right to further review.

The Audit Office will also, as required by the Privacy Act, notify the Privacy Commissioner of an application for internal review, keep the Privacy Commissioner informed of the progress of the review and inform the Privacy Commissioner of the findings of the review.

8.3 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 outcome of the internal review or is not satisfied with the action the Audit Office has taken, they have the right to apply to the NSW Civil Administrative Tribunal for a review of the conduct.

Further information about making an application to the tribunal is found on their [website](#). You can contact the tribunal at:

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

8.4 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 Privacy Commission in handling complaints is found on their website, www.ipc.nsw.gov.au. The contact details for the Privacy Commission are:

Email: ipcinfo@ipc.nsw.gov.au
Phone: 1800 472 679
Fax: 02 8114 3756
Post: GPO Box 7011, Sydney, NSW 2001

9 Contacting us

For more information about this plan or about the personal information we hold, please contact the Privacy Contact Officer:

Web: [Contact Us – Audit Office of New South Wales](#)
Email: governance@audit.nsw.gov.au
Phone: 02 9275 7100
Post: GPO Box 12, Sydney NSW 2001, Australia

10 Documentation and version

This version was reviewed in May 2016.

11 Appendix 1: privacy and personal information – definitions

11.1 Privacy

Privacy covers a number of things including:

- Information privacy – the way in which government agencies or organisations handle personal information such as age, address, physical or mental health records.
- Physical privacy – such as bag searching, use of DNA or fingerprints.
- Freedom from excessive surveillance – the right to go about our daily lives without being watched or have all our actions caught on camera.

11.2 Personal information

- Personal information is defined in both the Privacy Act and the Health Records Act.
- Personal information is defined in section 4 of the Privacy Act as:
 - information or an opinion...about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion
 - such things as fingerprints, retina prints, body samples or genetic characteristics.
- Personal information therefore can include a person's name, address, financial information or image.

11.3 Health information

- Health information is more specific and covers information or an opinion about a person's physical or mental health.
- Health information also includes personal information that is information or an opinion about:
 - a health service provided, or to be provided, to an individual
 - an individual's express wishes about the future provision of health services to him or her
 - other personal information collected in connection with the donation of human tissue
 - genetic information that is or could be predictive of the health of an individual or their relatives or descendants.

12 Appendix 2: Audit Office privacy related policies

- Code of Conduct
- Records Management Policy
- Secure Desk Policy
- Office Access Policy
- Information Security Policy
- Professional Independence Policy
- Privacy Policy for our website
- Working from Home Policy
- Social Media Policy.

13 Appendix 3: Other legislation

13.1 *Government Information (Public Access) Act 2009*

The *Government Information (Public Access) Act 2009* (the GIPA Act) focuses on making government information more readily available to the public. This means that the Audit Office must release information to the public unless there is an overriding public interest against doing so.

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 if the disclosure would:

- reveal an individual's personal information
- contravene an Information Protection Principle under the Privacy Protection Act or the Health Records Act.

In addition, the GIPA Act contains specific provisions relating to information collected during the audit process. Schedule 2 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 conclusively 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 us in response to a GIPA request.

13.2 *Public Finance and Audit Act 1983*

Section 38 of the *Public Finance and Audit Act 1983* provides that the Audit Office must preserve the secrecy of 'all matters and things' that are part of the information collected during the audit process.