



Privacy Management Plan

© 2015 State of NSW and Office of Environment and Heritage

Every effort has been made to ensure that the information in this document is accurate at the time of publication. However, as appropriate, readers should obtain independent advice before making any decision based on this information.

Published by:

Office of Environment and Heritage

59 Goulburn Street, Sydney NSW 2000

PO Box A290, Sydney South NSW 1232

Phone: +61 2 9995 5000 (switchboard)

Phone: 131 555 (environment information and publications requests)

Phone: 1300 361 967 (national parks, general environmental enquiries, and publications requests)

Fax: +61 2 9995 5999

TTY users: phone 133 677, then ask for 131 555

Speak and listen users: phone 1300 555 727, then ask for 131 555

Email: info@environment.nsw.gov.au

Website: www.environment.nsw.gov.au

Report pollution and environmental incidents

Environment Line: 131 555 (NSW only) or info@environment.nsw.gov.au

See also www.environment.nsw.gov.au

ISBN 978 1 74359 969 3

OEH 2015/0239

May 2015

Contents

1. Summary	1
2. Introduction	1
3. Objectives	1
4. Scope and application	2
5. Definitions	2
Personal information	2
Health information	2
Timeframe	3
6. Accessing or amending your information	3
7. Functions and information held by OEH	3
Protection of personal and health information – identity fraud	4
8. Information protection principles (IPPs)	4
8.1 Collecting personal information (IPPs 1-4)	4
8.2 Storing personal information (IPP 5)	5
8.3 Accessing personal information (IPPs 6-7)	5
8.4 Amending personal information (IPP 8)	6
8.5 Using personal information (IPPs 9-10)	6
8.6 Disclosing personal information (IPPs 11-12)	6
9. Health privacy principles (HPPs)	6
9.1 Collecting health information (HPPs 1-4)	7
9.2 Storing health information (HPP 5)	7
9.3 Accessing health information (HPPs 6-7)	7
9.4 Amending health information (HPP 8)	7
9.5 Using health information (HPPs 9-10)	7
9.6 Disclosing health information (HPP 11)	8
9.7 Identifiers (HPP 12)	8
9.8 Anonymity (HPP 13)	8
9.9 Transborder data flow to Commonwealth agencies (HPP 14)	8
9.10 Linkage of health records (HPP 15)	8
10. Exceptions to the PPIPA and HRIPA	9
10.1 Public registers	9
10.2 Directions of the Privacy Commissioner	9
10.3 Privacy code of practice	9
10.4 Other exemptions covered by the PPIPA or the HRIPA	9

11. Other privacy related legislation and policies	10
12. Complaints relating to how OEH has dealt with personal information	11
13. Promoting the plan	12
14. Accountabilities	12
14.1 Offences	12
14.2 Protection from liability	12
14.3 Responsibilities	13
15. Review	14
16. Contacts	14
Appendix 1 – OEH internal review procedures.....	15

1. Summary

This Privacy Management Plan (the Plan) is for the Office of Environment and Heritage (OEH), including the Environment Protection Authority (EPA), and shows what measures we take to ensure that we comply with the NSW *Privacy and Personal Information Protection Act 1998* (PPIPA) and the NSW *Health Records and Information Privacy Act 2002* (HRIPA) to protect the privacy of our clients, staff and others about whom we hold personal and health information.

It describes how members of the public can request access to and amendment of their personal and health information held by OEH and how we process an internal review or handle a complaint under the PPIPA or the HRIPA.

The EPA is a statutory corporation established under section 5 of the *Protection of the Environment Administration Act 1991*. OEH has entered into an agreement with the EPA to provide corporate and other essential services to the EPA. In addition, the EPA and OEH will mutually provide incidental services to support the delivery and expertise and/or regulatory, policy and other support.

All personal information collected, stored, used and disclosed by the EPA and OEH will be managed in accordance with this privacy management plan. The provision of information by the EPA and OEH in order to carry out functions as per the agreement, will be treated as confidential and will be used for the intended purpose only, in keeping with records management, policies, agreements and this plan.

2. Introduction

We take the privacy of our staff and clients seriously, and we will protect privacy with the use of this Plan as a reference and guidance tool.

The PPIPA and HRIPA contain principles on how to collect, store, access, amend, use and disclose personal and health information. The PPIPA covers personal information other than health information and requires OEH to comply with 12 information protection principles (IPPs). Health information includes information about a person's disability and health/disability services provided to them. There are 15 health privacy principles (HPPs) with which OEH must comply.

3. Objectives

The objectives of the plan are to:

- detail OEH's commitment to protecting the privacy rights of our clients, staff and others about whom we hold personal or health information
- inform employees about how to deal with personal and health information
- describe how individuals can request access to and/or amendment of their personal or health information
- integrate the IPPs and HPPs detailed in the PPIPA and the HRIPA into existing and future policies, guidelines and procedures that address information issues within OEH
- set procedures for internal review and how to handle complaints.

4. Scope and application

This plan applies to all staff engaged by OEH, whether by permanent appointment, temporary appointment, seconded from another agency, on work experience, volunteer work or as contractors.

A reference to OEH in this document also includes staff from the EPA.

5. Definitions

Personal information

Personal information is defined in the PPIPA as:

“information or an opinion about an individual whose identity is apparent or can be reasonably ascertained from the information or opinion”.

Personal information is information that identifies you and could be:

- a written record which may include your name, address and other details about you
- electronic records, photographs, images, video or audio footage and maps
- biometric information such as fingerprints, blood and records of genetic material.

The PPIPA excludes certain types of information. The most significant exemptions are:

- information contained in publicly available publications
- information about a person’s suitability for public sector employment
- information about people who have been dead for more than 30 years
- a number of exemptions relating to law enforcement investigations
- matters arising out of a Royal Commission or Special Commission of Inquiry
- matters contained in Cabinet documents.

Health information

Section 6 of the HRIPA defines ‘health information’ as:

- i) *personal information or an opinion about*
- *the physical or mental health or a disability (at any time) of an individual*
 - *an individual’s express wishes about the future provision of health services to him or her*
 - *a health service provided, or to be provided, to an individual*

or

- ii) *other personal information collected*
- *relating to provision of a health service*
 - *in connection with the donation of an individual’s body parts, organs or body substances*
 - *about genetic information pertaining to an individual arising from health service provision that could potentially predict the health of the individual or his/her relative.*

This privacy management plan refers to ‘personal information’, which in all instances includes health information, unless otherwise specified.

Timeframe

The legislation sets the following application timeframes for the IPPs and HPPs:

- personal information – collected since 1 July 2000; and
- health information – collected since 1 September 2004.

6. Accessing or amending your information

The types of personal and health information we hold about people is outlined in this plan. You can ask us to let you access and/or amend the personal or health information that we hold about you.

To make an access or amendment request, you should contact the business area holding the information (if known), or a Senior Governance Officer in the Privacy and Information Access team:

Phone: (02) 9995 6080 or 9995 6497

Postal Address: PO Box A290, Sydney South NSW 1232

Street Address: Level 14 59-61 Goulburn St, Sydney

Website: www.environment.nsw.gov.au/howeare/privacy.htm

7. Functions and information held by OEH

OEH has a range of functions requiring or involving the collection of personal information, including (but not limited to):

- consultation with the community, industry and other stakeholders
- identification, declaration and management of cultural and heritage sites
- investigation of complaints and allegations
- site audits
- incident management
- enforcement of environmental and conservation regulations
- issuing licences and permits
- energy efficiency initiatives with households and businesses
- sale of certain goods and services such as publications and park entry passes
- management of concessions (commercial or business activity) e.g. lease, franchise, easement within national parks
- management of volunteers
- conduct of apprenticeships and other training programs for members of the public
- provision of funding grants
- recommendation for awards

OEH holds document types that include personal and privacy related information. These fall within the following major categories:

- personnel, trainee and volunteer records and files
- incident reports
- application forms for licences, permits and grants
- complaints and reports of environmental and conservation incidents
- reports of investigations (e.g. research, audits, ethical conduct)

- public registers
- public submissions, feedback and comments
- databases of contractors and site auditors
- financial transactions for payment of goods and services delivered by OEH
- fines issued
- information agreements and other agreements entered into by OEH with its stakeholders and concession partners
- statutory declarations executed by members of the public to access public registers
- records of personal achievement for those being nominated for awards
- mailing lists
- subscriptions to OEH publications
- verbal/photographic/audio/video records provided to OEH about Aboriginal sites e.g. personal experiences relating to tradition and personal beliefs.

OEH holds health and personal records:

- relating to the firefighting capability of its staff as well as of volunteers
- relating to levels of exposure to radiation of certain staff members and health practitioners
- concerning most staff members, such as details about payroll, leave, training, workers compensation, medical certificates and similar/other personnel records.

Protection of personal and health information – identity fraud

When sending information by post, fax or email, OEH considers the risk of someone other than the intended recipient intercepting the correspondence and using the personal information contained in the document for identity fraud. To reduce this risk, personal information included in any correspondence (including attachments) will be kept to a minimum.

8. Information protection principles (IPPs)

The [Information Protection Principles](#) (IPPs) establish the legal obligations and standards for collecting and dealing with personal information to minimise the risk of misuse of that information.

There are 12 IPPs that are key to the PPIPA.

The degree of sensitivity of the personal information will influence the way in which the IPPs are applied. The more sensitive the nature of the information, the higher level of care that should be used by staff when dealing with such information, particularly where disclosure to a third party is being considered.

The key stages in the personal information management cycle are collection, storage, access, amendment, use and disclosure.

8.1 Collecting personal information (IPPs 1–4)

OEH collects personal information only for a lawful purpose that is directly related to its work, and is reasonably necessary for that work.

OEH takes reasonable steps to ensure that personal information it holds:

- is relevant to the purpose it has collected it for
- is not excessive

- is accurate, up-to-date and complete
- does not unreasonably intrude into the individual's personal affairs.

OEH collects personal information directly from the individual unless the individual has authorised someone else to give it to OEH; or, if the individual is under 16 years of age, the parent or guardian has provided it.

Some exceptions are in place to authorise public sector agencies, including OEH, to collect information from another public sector agency. These are outlined in section 10 of this Plan.

When collecting personal information, OEH explains:

- that personal information is being captured and the manner in which it is being collected
- why it is collecting the information
- the intended user/s and/or recipients of the information
- that personal information will not be disclosed or transferred without consent of the person concerned (unless otherwise lawfully authorised to do so)
- whether there is a legal requirement to give OEH the information, and what the consequences will be if the information is not provided. If there is no legal requirement, that the information is being collected voluntarily
- that owners of personal information have the right to access, modify and suppress their personal information.

In most cases OEH meets these requirements by including the necessary information on application or questionnaire forms used to collect the personal information.

OEH staff members (including managing contractors and consultants) responsible for designing forms, surveys or questionnaires, in web-based transactions or other instruments, ensure that they include adequate advice about OEH's privacy management procedures and OEH's contact details. OEH has a [commitment to privacy and security](#) specific to the OEH website and online newsletters.

8.2 Storing personal information (IPP 5)

OEH business units apply appropriate security to protect personal information. The security of information extends to all stages of the information life cycle, from the time of creation, while it is actively used, to archiving and destruction.

OEH does not keep personal information any longer than is necessary. Once personal information is no longer required, OEH staff ensure that it is securely disposed of and protected against misuse.

8.3 Accessing personal information (IPPs 6–7)

Owners of personal information held by OEH can [request to access](#) it (www.environment.nsw.gov.au/whoweare/access.htm). OEH provides access to the information without excessive delay or expense, usually within 30 working days. If there is likely to be a delay in providing the information, OEH will explain the delay and advise when the information is likely to be available.

If OEH refuses a request to access personal information under the PPIPA, it will provide detailed reasons. Alternatively, access to personal information can be requested under the *Government Information (Public Access) Act 2009*.

8.4 Amending personal information (IPP 8)

If you believe that the personal information held by OEH is inaccurate, irrelevant, not up to date, incomplete and/or misleading, you can [request that it be amended \(www.environment.nsw.gov.au/howeare/rules.htm#2\)](http://www.environment.nsw.gov.au/howeare/rules.htm#2).

OEH will determine whether it is appropriate to amend the personal information it holds within 30 working days of receiving a request. If OEH is not prepared to amend personal information, the reasons will be provided and OEH may instead attach a statement to the information indicating the amendment sought.

If your request for amendment is denied, you have rights of internal review under the PPIPA. See section 12 of this plan about complaints and internal reviews.

8.5 Using personal information (IPPs 9–10)

Before use, OEH ensures that personal information is accurate, up-to-date, relevant, complete and not misleading. This means that if some time has passed since the information was collected, or there is any other reason to have concerns about the information, OEH will take reasonable steps to check that it is still accurate, up-to-date, relevant, complete and not misleading.

OEH only uses personal information for the purposes for which it was collected. If there is a need to use the information for another purpose, the consent of the relevant individual is obtained. One exception to this is where the information is used to prevent danger to someone or in other specific situations set out in the PPIPA and outlined in section 10 of this Plan.

8.6 Disclosing personal information (IPPs 11–12)

OEH can disclose personal information to other parties for another purpose, other than the purpose the information was collected for, only if:

- the owner of the personal information agrees, or
- the owner of the personal information is aware that this sort of information is usually disclosed in the way it is being disclosed, or
- the secondary purpose is directly related to the purpose for which it was first collected, or
- information is supplied by OEH to prevent danger to someone.

This means that OEH staff do not provide the personal information of a person to a third party without that person's consent or in other specific situations set out in the PPIPA (refer section 10 of this Plan).

OEH does not disclose information relating to a person's ethnic or racial origin, political opinions, religious or philosophical beliefs or trade union membership, except to prevent death or injury.

OEH does not give personal information to anyone outside NSW unless there are similar privacy laws in that person's state or country or the disclosure is allowed under a privacy code of practice.

9. Health privacy principles (HPPs)

The HRIPA applies to OEH and how we protect health information that is held by OEH. It enables you to gain access to your own health information. There are 15 Health Privacy Principles (HPPs) listed in the HRIPA.

9.1 Collecting health information (HPPs 1–4)

OEH collects health information only for a lawful purpose that is directly related to its work, and is reasonably necessary to carry out its functions. The information is collected directly from the individual unless it is unreasonable or impracticable to do so. When we collect health information, we refer to the principles for the collection of personal information outlined above for IPPs 1–4.

If health information is collected from someone else, we ensure that you are made aware of this fact and have given your consent. The only time we do not follow these principles, is if making you aware would:

- pose a serious threat to the life or health of any individual, or
- the collection is made in accordance with guidelines issued by the Privacy Commissioner, or
- the HRIPA or other legislation provides an exemption

9.2 Storing health information (HPP 5)

OEH business units apply appropriate security to protect health information that they hold. The security of information extends to all stages of the information life cycle, from the time of creation, while it is actively used, to archiving and destruction.

9.3 Accessing health information (HPPs 6–7)

You can request access to your own health information held by OEH and we will tell you whether we hold any and if so, the nature of the information and the main purposes for which it is used. Access will be provided without excessive delay, usually within 45 days. If there is likely to be a delay in providing the information, OEH will explain the delay and advise when the information is likely to be available. A fee may be charged for providing a copy of your health information.

If OEH refuses your request to access health information, detailed reasons will be provided. Alternatively, access to health information can be requested under the *Government Information (Public Access) Act 2009*.

9.4 Amending health information (HPP 8)

If you believe that the health information held by OEH is inaccurate, irrelevant, not up to date, incomplete and/or misleading, you can [request that it be amended](#). You will need to provide evidence of your identity with your request for amendment.

OEH will determine whether it is appropriate to amend the health information it holds within 45 days of receiving a request. If OEH is not prepared to amend the health information, the reasons will be provided and OEH may instead attach a notation to the information indicating the amendment sought.

If your request for amendment is denied, you have right of internal review under the HRIPA. See section 12 of this plan about complaints and internal reviews.

9.5 Using health information (HPPs 9–10)

Before use, OEH ensures that the health information is accurate, up-to-date, relevant, complete and not misleading. This means that if some time has passed since the information was collected, or there is any other reason to have concerns about the information, OEH will take reasonable steps to check that it is still accurate, up-to-date, relevant, complete and not misleading.

OEH only uses health information for the purposes for which it was collected. If there is a need to use the information for another purpose, the consent of the relevant

individual is obtained. One exception to this is where the information is used to prevent danger to someone or in other specific situations set out in the HRIPA (refer section 10 of this Plan).

9.6 Disclosing health information (HPP 11)

OEH can disclose health information to other parties for another purpose, other than the purpose the information was collected for, only if:

- the owner of the health information agrees, or
- the secondary purpose is directly related to the purpose for which it was first collected, or
- information is supplied by OEH to prevent danger to someone, or
- the secondary purpose is reasonably necessary for the funding, management, planning or evaluation of health services or for training, research or for other reasons set out in the HRIP Act, or
- the exceptions set out in the HRIPA are established.

9.7 Identifiers (HPP 12)

OEH can assign identifiers to individuals if it is reasonably necessary to enable us to carry out our functions efficiently.

This identifier can in certain circumstances be adopted by a private sector person to carry out certain functions. The use and disclosure of an identifier can also be done if you have consented to it.

9.8 Anonymity (HPP 13)

Where it is lawful and practicable, people can obtain general information about OEH, without identifying themselves.

9.9 Transborder data flow to Commonwealth agencies (HPP 14)

OEH will only provide your health information to another person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency, where:

- it is a legal requirement and upholds the HPPs
- you consent to the transfer, or
- the transfer is necessary to do something you have requested, or
- the transfer is reasonably necessary to lessen or prevent serious and imminent threat to the life, health or safety of a person, or
- we have taken reasonable steps to ensure the HPPs will be complied with, or
- the transfer is permitted or required by legislation or law, or
- all of the following apply:
 - (a) the transfer is for your benefit, and
 - (b) it is impracticable to obtain consent from you, and
 - (c) if it were practicable to obtain consent, you would be likely to give it.

9.10 Linkage of health records (HPP 15)

We must not include your health information or disclose an identifier about you in a health linkage system unless you have expressly consented to the information being so included.

There may be times when we are lawfully authorised not to comply with HPP15, or where non-compliance is otherwise permitted under an Act or any other law, or the use complies with HPP 10(1)(f) and the disclosure complies with HPP 11(1)(f).

10. Exceptions to the PPIPA and HRIPA

10.1 Public registers

Under the PPIPA a public register is a register of personal information that is required by law to be, or is made, publicly available or open to public inspection. Information on public registers is only made available for legitimate purposes: that is a purpose relating to the purpose of the register or of the Act or legislation under which the register is kept.

OEH maintains a number of [public registers](#) and databases as required by legislation, e.g. *National Parks and Wildlife Act 1974*, *Threatened Species Conservation Act 1995* and *Wilderness Act 1987*. OEH also maintains the Aboriginal Heritage Information Management System (AHIMS) and the Historic Heritage Information Management Systems (HHIMS). These registers are located on the OEH website.

The EPA also maintains public registers (see www.epa.nsw.gov.au/publicregister/).

Any person whose personal and privacy information is recorded in an OEH register has the right to request that their personal details be suppressed. This is to protect people whose position or occupation requires a high level of personal security or people who have well-founded fears of violence or harm, e.g. victims of domestic violence, police informants, judges, senior police officers.

10.2 Directions of the Privacy Commissioner

Under section 41 of the PPIPA and section 62 of the HRIPA, the Privacy Commissioner may make a direction to waive or modify the requirement for a public sector agency to comply with an information protection principle, a health privacy principle or a privacy code of practice.

Three current directions have specific relevance for OEH's operations. They relate to:

- disclosure of information by public sector agencies for research purposes
- information transfers between public sector agencies
- direction on processing of personal information by public sector agencies in relation to their investigative functions.

Copies of these section 41 directions can be found on the Information and Privacy Commission website: www.ipc.nsw.gov.au/public-interest-directions.

10.3 Privacy code of practice

Under the PPIPA, codes of practice may be created to allow an agency to modify the application of one or more information protection principles or specify how they are to be applied to particular activities or classes of information. The *Privacy Code of Practice (General) 2003* applies to the EPA.

10.4 Other exemptions covered by the PPIPA or the HRIPA

It is worth noting that both the PPIPA and the HRIPA provide some specific exemptions from the IPPs and the HPPs.

Some of the exemptions in the PPIPA are listed in sections 22–28 and include:

- law enforcement and related matters

- investigative agencies
- where lawfully authorised or required
- when it would benefit the individual concerned
- Minister being informed of certain matters.

Each of the HPPs in the HRIPA lists certain circumstances in which OEH is not required to comply with a requirement. Some of these include:

- where lawfully authorised or required
- where non-compliance is otherwise permitted under an Act or any other law
- there is a serious threat to health or welfare
- the use for a secondary purpose, such as management of health services, training and/or research will only be done where it is not possible to carry out that purpose using de-identified information and it is not reasonably practicable to seek your consent.
- finding a missing person
- suspected unlawful activity or conduct grounds for disciplinary action.

Lastly, you may give us consent to not comply with any or some of the IPPs or the HPPs in particular circumstances.

11. Other privacy related legislation and policies

The key legislation, policies and procedures relevant to OEH include:

Anti-Discrimination Act 1977

Crimes Act 1900

Government Information (Public Access) Act 2009

Public Interest Disclosures Act 1994

State Records Act 1998

Telecommunications (Interception and Access) (New South Wales) Act 1987

Workplace Surveillance Act 2005

Other legislation that may affect or impact on personal and/or health information:

National Parks and Wildlife Act 1974

Native Vegetation Act 2003

Threatened Species Conservation Act 1995

Wilderness Act 1987

Environmental Planning and Assessment Act 1979

Industrial Relations Act 1996

Contaminated Land Management Act 1997

Dangerous Goods (Road and Rail Transport) Act 2008

Environmentally Hazardous Chemicals Act 1985

Forestry Act 2012

National Environment Protection Council (New South Wales) Act 1995

Ozone Protection Act 1989

Pesticides Act 1999

Protection of the Environment Administration Act 1997

Protection of the Environment Operations Act 1997

Radiation Control Act 1990

Recreational Vehicles Act 1983

Waste Avoidance and Resource Recovery Act 2001

The above listed legislation can be found on the NSW Legislation website:

www.legislation.nsw.gov.au/maintop/scanact/inforce/NONE/0

Related OEH policies as issued from time to time:

- [Agency Information Guide \(GIPA Act\)](#)
- [Code of Ethical Conduct](#)
- [Network Acceptable Use Policy](#) (intranet only)
- [Public Interest Disclosures Policy and Procedures](#) (intranet only)

When new policies, procedures and guidelines are devised, reference must be made to this plan to ensure compliance with the PPIPA and the HRIP Act. Contact the Program Leader – GIPA/Privacy or the Right to Information/Privacy Officer in the Group Coordination and Governance Branch, for assistance and advice.

12. Complaints relating to how OEH has dealt with personal information

If you believe that OEH may have breached your privacy, you can raise an informal complaint, lodge a formal complaint or submit an application for internal review of conduct with OEH. A complaint can also be lodged with the [Information and Privacy Commission](#).

If you want to resolve an issue informally, please contact the relevant area of OEH, if known, to discuss your issue. Informal complaints may be handled under the 'Guidelines for managing external complaints and allegations', if appropriate. Your complaint may be referred for an internal review to be carried out, if it is considered that a serious breach of privacy has occurred, or that it is more appropriate to deal with your complaint on a formal basis.

Under the formal process you can have the decision reviewed by the Privacy Commissioner or the Administrative and Equal Opportunity Division of the NSW Civil and Administrative Tribunal, whereas informal complaints are dealt with by officers within OEH and there are no formal review rights.

Under the HRIPA and PPIPA, [complaints or applications for internal review](#) to OEH:

- should be lodged within six months of becoming aware that OEH has handled personal and/or health information in an inappropriate manner
- should be in writing ([a form is available from the OEH website](#))
- must have a return address in Australia.

An internal review is conducted by a senior officer who was not substantially involved in the matter being complained about. This officer is responsible for reviewing the action or decision and deciding if it is correct. There is no cost to lodge a complaint or request an internal review. Reviews must be completed within 60 days. A copy of the [application form for a privacy complaint and internal review](#) is located on the OEH website.

OEH's internal review process is set out in Appendix 1.

If an applicant is not satisfied with the result or the process of an internal review, the applicant can complain to the [Information and Privacy Commission](#) (IPC). The IPC can be contacted on 1800 472 679.

Appeals may also be lodged with the [Administrative and Equal Opportunity Division of the NSW Civil and Administrative Tribunal](#) (NCAT) within 28 days after receiving the report from the IPC. If OEH does not complete the internal review within 60 days, then an appeal may be lodged with NCAT 28 days after the request for an internal review was lodged with OEH. The NCAT can be contacted on 1300 006 228.

13. Promoting the plan

OEH employs the following broad strategies to ensure ongoing compliance with the privacy legislation:

- As part of OEH's induction program, new staff are provided with information to raise their awareness and appreciation of the privacy legislation requirements.
- OEH provides refresher and on-the-job training for specialist staff.
- OEH highlights the Privacy Management Plan during the annual Privacy Awareness Week.
- Where OEH proposes to collect personal information on forms, questionnaires, survey templates, interview sheets, etc., these are reviewed by the responsible managers to ensure compliance with privacy principles.
- When existing tools for collecting personal information are updated, managers review them to ensure compliance with privacy principles.
- The Governance Branch provides specialist advice relating to the interpretation and practical implementation of the privacy legislation.
- The Privacy Management Plan is published on the OEH website.
- The Privacy Management Plan is reviewed and updated every two years.
- Every five years OEH formally reviews its compliance with the privacy legislation. This was last undertaken in 2007.

14. Accountabilities

All staff have a duty to act in accordance with this plan. If staff feel uncertain as to whether certain conduct may breach their privacy obligations, they should seek advice from the Privacy and Information Access Team.

14.1 Offences

It is a criminal offence, punishable by up to two years' imprisonment, for any employee (or former employee) of OEH to intentionally use or disclose any personal information about another person, to which the employee has or had access in the exercise of his or her official functions, except as necessary for the lawful exercise of his or her official functions.

[Part 8 of the PPIPA](#) and [part 8 of the HRIPA](#) provide further details about offences in respect of personal and health information.

14.2 Protection from liability

[Part 8 of the PPIPA](#) and [part 8 of the HRIPA](#) provide certain protections from liability where a person has acted in good faith.

14.3 Responsibilities

Positions with significant responsibilities are:

Position	Responsibility
Chief Executive and Executive	<ul style="list-style-type: none"> • Establish and maintain policies, systems and procedures for all aspects of privacy management. • Ensure mechanisms for responding to critical issues or risks arising are appropriate and effective. • Ensure areas of work that are of inherently higher risk are identified and that preventive strategies are in place. • Make the Privacy Management Plan publicly available. • Confirm support for privacy compliance in the Code of Ethical Conduct.
Managers and supervisors	<ul style="list-style-type: none"> • Make staff aware of this plan and help them to use it. • Ensure staff are provided with access to privacy training and other development possibilities. • Identify privacy issues when implementing new systems. • Provide feedback regarding the effectiveness of the plan and suitable refinements to the Governance Branch as necessary.
Governance Branch OEH Privacy and Information Access Team OEH	<ul style="list-style-type: none"> • Reinforce compliance with privacy legislation. • Report on privacy issues in the annual report. • Advise and assist staff and the public in responding to requests for information. • Support the plan through awareness-building, skills development and user training. • Help staff by providing advice and assistance if clarification regarding the plan is required. • Monitor the effectiveness of the plan and propose suitable refinements where appropriate.

15. Review

The Governance Branch is responsible for coordinating review of the plan. Reviews will be undertaken at least every two years and more frequently if changes in legislation, policies or other areas require amendment of the plan.

The next scheduled review is due in 2017.

16. Contacts

For information relating to this plan or how to request information under the PPIPA, HRIPA or the *Government Information (Public Access) Act 2009*, or how to ask for amendment of personal or health information, contact the **Privacy and Information Access Team**:

Phone: (02) 9995 6080, 9995 6497 or 9995 6297

Postal Address: PO Box A290, Sydney South NSW 1232

Street Address: Level 14 59-61 Goulburn St, Sydney

Website: [OEH and your privacy | NSW Environment and Heritage](http://www.environment.nsw.gov.au/whoweare/privacy.htm)
(www.environment.nsw.gov.au/whoweare/privacy.htm)

Advice on the PPIPA, HRIPA and the *Government Information (Public Access) Act 2009* is also available from the **Information and Privacy Commission**:

Phone: 1800 472 679

Email: ipcinfo@ipc.nsw.gov.au

Postal Address: GPO Box 7011, Sydney NSW 2001

Street Address: Level 11, 1 Castlereagh St, Sydney

Website: www.ipc.nsw.gov.au

Appendix 1 – OEH internal review procedures

Any complaint or request for an internal review in relation to a privacy matter is to be forwarded to the [Privacy and Information Access Team](#).

A senior reviewing officer will be allocated and will:

Step 1: Assess the application to confirm that:

- it is about personal information in relation to conduct that occurred after 1 July 2000, or
- it is about health information in relation to conduct which occurred after 1 September 2004, and
- it has been lodged within 6 months of the applicant becoming aware of the alleged conduct.

If the application does not meet these criteria it will be referred to relevant managers for handling under OEH's normal [complaint handling procedures](#). If the criteria are met, the reviewing officer will proceed with the following steps.

Step 2: Write to the applicant within 14 days of receiving the application stating:

- the officer's understanding of the conduct complained about
- the officers understanding of the privacy principle/s at issue
- that OEH is conducting an internal review under the NSW *Privacy and Personal Information Protection Act 1998* and/or the NSW *Health Records and Information Privacy Act 2002* as appropriate
- the reviewing officer's name, title and contact details
- how the reviewing officer is independent of the person/s responsible for the alleged conduct
- the estimated completion date for the review process
- that if the review is not completed within 60 days of the date the application for review was received, the applicant can go to the [Administrative and Equal Opportunity Division of the NSW Civil and Administrative Tribunal](#) (NCAT) for an external review of the alleged conduct
- that a copy of the letter will be provided to the [Privacy Commissioner](#) who has an oversight role.

Step 3: Send a copy of this letter to the Privacy Commissioner.

Step 4: Review the situation to determine whether the conduct occurred, and if so whether it constituted an unauthorised breach of the relevant privacy legislation.

Step 5: Should the review not be finalised within four weeks of the issuing of the letters at steps 2 and 3 above, **send a progress report** to the applicant, copied to the Privacy Commissioner:

- detailing progress to date
- advising of any anticipated delays, the reasons for these, and a revised estimated completion date for the review process
- a reminder that if the review is not completed within 60 days of the date the application for review was received the applicant can go to NCAT for an external review of the alleged conduct

Step 6: On completion of the review, write a draft report:

- detailing the review findings about the facts of the matter, the law and the reviewer's interpretation of the law
- setting out a determination as to whether a breach has occurred, with one of the following findings:
 - insufficient evidence to suggest alleged conduct occurred
 - alleged conduct occurred but complied with the privacy/health privacy principles and/or public register provisions
 - alleged conduct occurred, but the non-compliance was authorised by an exemption, Code or Direction (s.41 of PPIPA / s.62 of HRIPA)alleged conducted occurred: conduct did not comply with principles or public register provisions and was not authorised, so constitutes a "breach" of the legislation
- making recommendations on appropriate OEH action by way of response or remedy.

Step 7: Provide a copy of the draft report to the Privacy Commissioner for comment, and check whether the Commissioner wishes to make a submission

Step 8: Finalise the report, and submit to the Chief Executive for endorsement.

Step 9: Notify the complainant and the Privacy Commissioner in writing:

- that review is finished
- of the review findings (and the reasons and legislative basis for those findings), and the action proposed to be taken
- of the right to complain to the Information and Privacy Commission (IPC), providing contact details for the IPC.
- of the right to apply within 28 days to the Administrative and Equal Opportunity Division of the NSW Civil and Administrative Tribunal for a further review, providing contact details for the Tribunal.