Privacy Management Plan

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

OEH 2017/0267
June 2017

Find out more about your environment at:

www.environment.nsw.gov.au

Contents

Document control

Author:	Manager, Privacy and Information Access Office of Environment and Heritage Planning and Environment Cluster
Date of original endorsement:	11/12/2013
Date of effect:	01/01/2014
Date last modified:	May 2017
Date for review:	2019
Document version number:	3

This Privacy Management Plan has been updated to reflect changes in legislation and additional tools for staff to better manage privacy obligations.

The Plan has been expanded since the last version, to also include information about:

- Intra-governmental flows of information for data analytics purposes
- Transborder disclosures
- Privacy Impact Assessments
- Workplace surveillance
- Data breach notifications

In addition, the updated Plan has been prepared in a more generic manner so that each agency within the Planning and Environment Cluster can readily adopt it, by adding their specific details to Appendix 4.

1. Summary

This Privacy Management Plan (the Plan) was prepared by the Office of Environment and Heritage (OEH) with input from the Department of Planning and Environment (DPE) and the Environment Protection Authority (EPA). It has been made available to all agencies within the Planning and Environment cluster. Agencies within the cluster that have adopted the Plan are:

- Centennial Park and Moore Park Trust
- Department of Planning and Environment
- Environment Protection Authority
- Environmental Trust (NSW)
- Greater Sydney Commission
- Hunter Development Corporation
- Jenolan Caves Reserve Trust
- Joint Regional Planning Panels
- Office of Environment and Heritage
- Royal Botanic Gardens and Domain Trust

Further details of each of these agencies can be found at Appendix 4.

The Plan shows what measures the adopting agencies take to 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.

This Plan has been prepared and implemented as required under section 33 of the PPIPA. We may amend this Plan from time to time, as required, by changes in legislation, processes, procedures or other events.

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

Where this Plan mentions the words ‘us’, ‘we’ and ‘our’, they refer to the agencies that have adopted this plan.

2. Introduction

We take the privacy of our staff and clients seriously, and we will manage and protect personal information 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 us 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 we must also comply.

3. Objectives

The objectives of the plan are to:

- detail our commitment to protecting the privacy of our clients, staff and others about whom we hold personal or health information
- inform our employees about how to manage and protect personal and health information
- describe how you can request access to and/or amendment of your personal or health information, held by us
- integrate the IPPs and HPPs into existing and future policies, guidelines and procedures that address information issues
- set complaint handling and internal review procedures
- inform you on how to request an internal review
- explain the right for you to apply to the NSW Civil and Administrative Tribunal, in cases where you remain dissatisfied with internal review findings.

4. Scope and application

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

Timeframe

The legislation sets the following timeframes:

- For the IPPs, personal information collected since 1 July 2000; and
- For the HPPs, health information collected since 1 September 2004.

5. Definitions

Personal information is defined in section 4 of 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 provisions that could potentially predict the health of the individual or his/her relative.

This Plan refers to 'personal information', which in all applicable instances includes health information, unless otherwise specified.

6. Accessing or amending your information

The types of personal information we hold about people is outlined in this plan. You can ask us for access to and/or amendment of your personal 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 contact the relevant privacy officer of the agency.

Further details about amending personal information is covered in section 8.4.

Appendix 4 contains the relevant contact details of each agency.

7. Functions and information held

We have a range of functions requiring or involving the collection and use of personal information. These are outlined for each agency at Appendix 4.

The major categories of document types that we hold that may include personal and privacy related information is also outlined in Appendix 4.

Protection of personal and health information – identity fraud

When sending information by post, fax or email, we consider 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) is kept to a minimum.

Information made digitally available, to conform with open government principles, or otherwise, to make information available, will be de-identified, anonymised or redacted to remove any personal identifying information of individuals.

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. The final stage is ensuring that information is destroyed when no longer required for the purpose for which it was collected.

8.1 Collecting personal information (IPPs 1-4)

We collect personal information only for a lawful purpose that is directly related to our work, and is reasonably necessary for that work. There are a number of ways that this is collected:

1. Provided through direct actions that you are fully aware of. For example, registering on our website, applying for a licence or informing us of an allegation, complaint or issue. You may also pay by credit card for a service, take a test or respond to questions or surveys. Information provided to us, is usually with your knowledge. It is our preferred way to collect your personal information.
2. Observed information may be recorded in our records, as relevant to information provided. This could include details from online cookies, CCTV footage in public places (if combined with facial recognition).
3. Derived data is that which is mechanically collected, such as the number of times a website is visited, how often a service is requested or some other arithmetic process used on current data to predict future required services.
4. The final way that information may be collected is inferred. This may occur where statistical information is based on current personal information held by us. For example, it could include response scores, number of services requested, or in some project where big data is being used to generate insights into future needs.

Of the four methods of collection above, you may only be aware of the first one, where information has been provided by you. You may be aware of observed information and even derived data. However, it is unlikely you would know about the inferred information and it is likely that inferred information would be so de-identified, it would be impossible to specifically identify you.

All of the above methods of collecting are possible, but may not all be used by us. They are included in this plan to make you and us aware of the way that information may be collected and as a reminder to us to be careful to manage such information properly.

We take reasonable steps to ensure that personal information we hold:

- is relevant to the purpose we have collected it for
- is not excessive
- is accurate, up-to-date and complete
- does not unreasonably intrude into the individual’s personal affairs.

We collect personal information directly from you, unless you have authorised someone else to give it to us; or, if you are under 16 years of age, your parent or guardian has provided it.

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

When collecting your personal information, we explain:

- that personal information is being captured and the manner in which it is being collected
- why we are collecting the information
- the intended user/s and/or recipients of the information
- that your personal information will not be disclosed or transferred without your consent (unless otherwise lawfully authorised to do so)
- whether there is a legal requirement to give us 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 you have the right to access, modify and suppress your personal information.

In most cases we meet these requirements by including a privacy statement containing the necessary information on application or questionnaire forms used to collect the personal information or on our website when seeking submissions.

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 our privacy management procedures and our contact details.

We have a commitment to privacy and security specific to our website and online newsletters. Each agency's website can be found in Appendix 4.

8.2 Storing personal information (IPP 5)

Each of our 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.

We have an ICT policy, use passwords and, where possible, encrypt information to ensure it is protected and kept secure. All staff must comply with the Code of Ethics and Conduct and are provided with training on privacy.

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

The Records Management Policy and the *State Records Act 1998* provide guidance on how to do this. The Retention and Disposal Authority relevant to a particular record will be followed. For example record relating to compensation claims, financial management or industrial relations is kept for a minimum of seven years after action completed.

8.3 Accessing personal information (IPPs 6-7)

If you wish to know whether we hold personal information about you, you can contact us directly to enquire. We will be able to tell you whether we hold your personal information, the nature of the personal information we hold and the main purposes for which the personal information is used. Contact details for agencies are listed in Appendix 4.

If you wish to gain access to your own personal information held by us, you can request access to it. Access will be provided without excessive delay or expense, usually within 20-30 working days, of receiving a request. If there is likely to be a delay in providing the information, we will explain the delay and advise when the information is likely to be available.

Each business area that holds personal information has appropriate processes in place to allow people to access their own personal information.

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

Section 5 of the PPIPA and section 22 of the HRIPA states that nothing in the PPIPA or HRIPA affects the operation of the GIPA Act. This means that the PPIPA and the HRIPA do not override the GIPA Act or lessen any obligations under the GIPA Act in respect of a public sector agency.

Appendix 4 provides the contact details of each agency covered by this Plan. You can also apply directly to the relevant business area holding your information, if you know it.

8.4 Amending personal information (IPP 8)

If you believe that your personal information held by us is inaccurate, irrelevant, not up to date, incomplete and/or misleading, you can request that it be amended.

You need to demonstrate that the information you want amended is in fact inaccurate, irrelevant, not up to date, incomplete and/or misleading. Some kind of evidence will need to be provided to support your claim.

See Appendix 4 for contact details of where to send your request.

We will determine whether it is appropriate to amend the personal information we hold within 20-30 working days of receiving a request. If we are not prepared to amend personal information, the reasons will be provided and we may instead attach a statement to the information indicating your requested amendment.

If your request for amendment is denied, you have rights of internal review under the PPIPA. See section 14 of this plan about complaints and internal reviews.

8.5 Using personal information (IPPs 9-10)

Before use, we ensure 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 adequacy of the information, we will take reasonable steps to check that it is still accurate, up-to-date, relevant, complete and not misleading.

We only use your personal information for the purposes for which it was collected. If there is a need to use the information for another purpose, we are required to ask for your consent. 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)

We 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 us to prevent danger to someone.

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

We do 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.

We do 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, or under legislation (such as HRIPA and PPIPA). We may also disclose information if the disclosure will benefit you, it is impracticable to obtain your consent, and if we could obtain your consent it is likely you would give it.

There are secrecy provisions in various legislation. Section 11 of the GIPA Act overrides those provisions.

9. Health privacy principles (HPPs)

The HRIPA applies to how we protect health information that is held by us. 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)

We collect health information only for a lawful purpose that is directly related to our work, and is reasonably necessary to carry out our functions. The information is collected directly from you 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)

Our 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)

If you wish to know whether we hold health information about you, you can contact us directly to enquire. We will be able to tell you whether we hold your health information, the nature of the health information we hold and the main purposes for which the health information is used. Contact details for agencies are listed in Appendix 4.

You can request access to your own health information held by us 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 20 days and never longer than 45 days. If there is likely to be a delay in providing the information, we 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 we refuse 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.

Our contact details are listed at Appendix 4.

9.4 Amending health information (HPP 8)

If you believe that the health information held by us 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, as well as details supporting that the information you want amended is in fact inaccurate, irrelevant, not up to date, incomplete and/or misleading.

We are required to determine whether it is appropriate to amend the health information we hold within 45 days of receiving a request. If we are not prepared to amend the health information, the reasons will be provided and we may instead attach a notation to the information indicating the amendment you have sought.

If your request for amendment is denied, you have right of internal review under the HRIPA. See section 14 of this plan about complaints and internal reviews.

9.5 Using health information (HPPs 9-10)

Before use, we ensure 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 adequacy of the information, we will take reasonable steps to check that it is still accurate, up-to-date, relevant, complete and not misleading.

We only use health information for the purposes for which it was collected. If there is a need to use the information for another purpose, your consent 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)

We 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 us 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 HRIPA; or
- the exceptions set out in the HRIPA are established.

See section 10 of this Plan for more details.

There are secrecy provisions in various legislation. Section 11 of the GIPA Act overrides those provisions.

9.7 Identifiers (HPP 12)

We 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, you will be given an opportunity to retain your anonymity when entering into transactions with us.

9.9 Transborder data flow to outside NSW or to the Commonwealth (HPP 14)

We 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, or
- 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. Modifications 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 reason for of the register to exist, or of the Act or legislation under which the register is kept.

We maintain a number of public registers and databases as required by legislation (see Appendix 3).

Any person whose personal information is recorded in a 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, and/or senior police officers. If you want your personal information that is contained in a public register suppressed contact us to make an application. The contact information for agencies is at Appendix 4.

The EPA is specifically covered by the *Privacy Code of Practice (General) 2003* (the Code) in respect of modification of part 6 of the PPIPA and the registers kept by the EPA. Schedule 2 of the Code, limits the information required to be published on the registers in respect of various legislation that the EPA operates under.

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.

Agencies can approach the Privacy Commissioner to request a Direction. The general intent is for the Directions to apply temporarily. If a longer term waiver or in the application of an IPP or HPP, then a Code of Practice may be more appropriate.

As of 1 January 2016, some previous Directions have been incorporated into legislation, including the PPIPA. Directions currently in operation are listed on the website of the Privacy Commissioner (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 in respect of environmental offences involving vehicles (Schedule 1).

This means the EPA may contact the owner (operator) of a vehicle when it has received a report about an environmental offence concerning the vehicle. The Roads and Traffic Authority (currently known as Roads and Maritime Services) may exchange the vehicle registered operator details with the EPA for this purpose.

10.4 Some 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 (section 23)
- investigative agencies (section 24)
- where lawfully authorised or required (section 25)
- when it would benefit the individual concerned (section 26)
- specific exemptions in relation to ICAC, NSW Police Force, PIC and the NSW Crime Commission (section 27)
- exchanges between public sector agencies (section 27A)
- research (section 27B)
- credit information (section 27C)
- other exemptions (section 28).

Each of these exemptions are outlined further below.

10.4.1 Law enforcement and related matters

Section 23 of the PPIPA provides exemptions relating to law enforcement and related matters. The Privacy Commissioner has advised that section 23(3) should be read ‘as referring to information (collected about) a specific incident or incidents involving a breach of the criminal law … (not) the collection of personal information that may potentially have some law enforcement use in the future’.

The term ‘law enforcement purposes’ refers only to criminal law enforcement, not breaches of professional standards or misconduct.

Section 23(4) mentions ‘public revenue’, which the Privacy Commissioner has indicated to mean ‘a function of collecting income on behalf of the government … (not) merely saving expenditure. Collection of stamp duty should be considered as included, but it is less clear if the collection of income by way of fines, or government charges for services would be included’.

10.4.2 Investigative agencies

Section 3 of the PPIPA defines certain terms, including investigative agencies, where certain agencies are named, such as the Ombudsman’s Office and ICAC. It also covers any other NSW public sector agency with investigation functions, if those functions are exercisable under the authority of an Act or statutory rule and it may result in the agency taking or instituting disciplinary, criminal or other formal action or proceedings against a person or body under investigation.

10.4.3 Lawfully authorised

The term ‘lawfully authorised’ used in section 25 of the PPIPA has been covered by various tribunal matters and has been identified to include a number of issues, such as (not a limited list, just examples):

- Disclosure within the terms of a subpoena
- Requirement to notify a person against whom a complaint has been made
- Inform a union official in respect of various issues under legislation
- Disclosures to Anti-Discrimination Board, or other such boards or commissions.

Although certain requirements under legislation would appear to allow for the disclosure of personal information, care must be taken by staff and an assessment made to only divulge the minimum amount of information required.

10.4.4 Benefit the individual

Section 26 provides an exemption where non-disclosure would prejudice the interests of the individual to whom the information relates or there has been express consent for another use or disclosure.

Consent is only genuine if you have the capacity to give or withhold consent. For consent to be valid it must be voluntary, informed, specific and current. Notifying you of what we intend to do with your personal information is not express consent.

10.4.5 Exchanges of information between agencies

Section 27A of the PPIPA provides an exemption relating to information exchanges between public sector agencies. Information can be provided to or by another public sector agency, if it is reasonably necessary:

- To allow any of the agencies concerned to deal with, or respond to, correspondence from a Minster or Member of Parliament, or
- To enable inquiries to be referred between the agencies concerned, or
- To enable the auditing of the accounts.

This may occur where an application for a service has been submitted to one agency and the actions of another agency is needed to provide a response.

Staff, should seek consent from the person involved, if possible, and/or ask for advice from the relevant agency’s privacy expert (see Appendix 4).

10.4.6 Research

There are many definitions of research. It can be a systematic investigation to establish facts, principles or knowledge or a study to obtain or confirm knowledge. A defining feature of research is the validity of its results. The knowledge that is generated by research is valid in the sense that what is discovered about particular facts investigated can be justifiably claimed to be true for all like facts.

Privacy Commissioners around Australia agree that research is ‘an activity that goes beyond simply meeting the needs of the organisation conducting the activity, by offering some form of wider community benefit’. That is, the research activity should be in the public interest.

10.4.7 Other exemptions

The other exemptions under section 28 of the PPIPA relate to various agencies named in section 28(1), Multicultural NSW in section 28(2) and an exemption for any public sector agency if the disclosure is to inform the Minister or the Premier about any matter within their administration (section 28(3) of the PPIPA).

These exemptions should only be relied on after seeking advice. See Appendix 4.

10.4.8 Exemptions under the HRIPA

Each of the HPPs in the HRIPA lists certain circumstances in which we are not required to comply with the principles. 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. Data Analytics Centre and sharing information

The *Data Sharing (Government Sector) Act 2015* (DSGS Act) was created to promote sharing of information for certain purposes which include allowing the government to carry out data analytics for the purposes of identifying issues and solutions to better develop government policy, program management, and service planning and delivery.

The DSGS Act provides for the expeditious sharing of information with the Data Analytics Centre (DAC), which operates within the Department of Finance, Services and Innovation, or between other government sector agencies. It also provides protections in connection with data sharing and ensures compliance with the requirements of PPIPA and HRIPA for privacy protection.

We are required to ensure that health and/or personal information contained in the data that is shared complies with privacy legislation. We are also obliged to ensure that any confidential and commercial-in-confidence information contained in the data to be shared complies with any contractual or equitable obligations of the data provider concerning how it is dealt with.

Before responding to a request from DAC to provide information, we consult internally with the privacy expert (staff member) to obtain relevant advice (see Appendix 4). We may also ask the Privacy Commissioner to guide us on the best way to comply with the request for information whilst upholding the IPPs and HPPs.

12. Requests for information from other agencies

We may receive a request from another agency, such as NSW Police, the Ombudsman's Office, ICAC or others. When such a request is received we ask for it in writing, on letter-head (or email with adequate details to identify the agency) and for the request to nominate a contact person.

Before releasing information to the other agency, we check the named legislation relied upon for the provision of information and ensure the request is legitimate. This is often done by contacting the nominated officer by telephone.

If in any doubt as to the legitimacy of the request, we check internally with our privacy expert or contact the agency that asked for the information.

13. Transborder flows of personal information

Section 19(2) of the PPIPA provides additional requirements to disclosure of information outside of New South Wales. Where information needs to be disclosed to a recipient outside the NSW jurisdiction or to a Commonwealth agency, there are some additional criteria to be met. These depend on the type of information and are set out in the Guidance provided by the Office of the Privacy Commissioner.

Before any personal information is disclosed outside of NSW, we make enquiries with the recipient to ensure they have similar privacy laws. We draw up a contract that meets the requirements of section 19(2) of the PPIPA. We may also seek legal advice.

14. Other privacy related legislation and policies

The key legislation, policies and procedures relevant to privacy are listed in Appendix 7 of this Plan. The legislation in Appendix 7 is not a complete list. However, it does provide an overview of the types of laws that may affect your personal information.

In our policies, procedures and guidelines, we are required to make reference to this plan to ensure compliance with the PPIPA and the HRIPA.

15. Complaints and internal reviews

If you believe that we may have breached your privacy, or have not complied with a request for access or amendment, you can:

- raise an informal complaint, or
- submit an application for internal review of conduct with us.

A complaint can also be lodged with the Information and Privacy Commission. The Privacy Commissioner may only make recommendations and does not investigate complaints regarding alleged conduct of public sector agencies where the Internal Review mechanism is available. The investigative functions may result in an investigation report or conciliation of a complaint. The Privacy Commissioner's functions do not result in binding outcomes.

If you want to resolve an issue informally, please contact the relevant area, if known, to discuss your issue. Informal complaints may be handled under relevant 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 Administrative and Equal Opportunity Division of the NSW Civil and Administrative Tribunal. By contrast, informal complaints are dealt with by our officers and there are no formal review rights.

Under the HRIPA and PPIPA, complaints or applications for internal review to us:

- should be lodged within six months of becoming aware of the legal implications/ significance of the alleged conduct
- should be in writing (a form is available from our website, but is not necessary)
- 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 our website.

See Appendix 4 for the relevant website address.

Our internal review process is set out in Appendix 1. Please note that the Privacy Commissioner may make recommendations in respect of the process.

If you are unhappy with the result of an internal review, you can appeal to the Administrative and Equal Opportunity Division of the NSW Civil and Administrative Tribunal (NCAT). Appeals may be lodged with the NCAT within 28 days after receiving the report. If we do not complete the internal review within 60 days, then an appeal may be lodged with NCAT within 28 days after you were due to receive the report. The NCAT can be contacted on 1300 006 228.

16. Privacy Impact Assessment

A Privacy Impact Assessment (PIA) may be required to assess any actual or potential effects that an activity, project or proposal may have on personal information held by us. A PIA can also outline ways in which any identified risks can be mitigated and any positive impacts enhanced.

Public consultation and measuring community expectations is an important part of any thorough PIA. A PIA should examine both the positive (privacy-enhancing) and negative (privacy-invasive) impacts, but primarily focus will be on the negative impacts and how to address such risks.

Privacy risks can be avoided or mitigated by:

- ensuring a project complies with the law,
- ensuring a project meets community expectations,
- making a project less privacy-invasive, and
- making a project more privacy-enhancing.

It may not be possible to eliminate or mitigate every risk, but ultimately a judgement will be made as to whether the public benefit to be derived from the project will outweigh the risk posed to privacy.

To know if a PIA is required, staff should refer to Appendix 2, which sets out a checklist with some simple yes/no questions. If the answer to one of more of those questions is “yes”, then advice should be sought from the privacy expert in the agency and a PIA should be seriously considered.

There are many benefits in carrying out a PIA, such as:

- Helps to ensure compliance with privacy legislation
- Helps reduce costs later in management time, legal expenses and potential media or public concern by considering privacy issues early
- Assists in anticipating and responding to the public’s possible privacy concerns
- Enhances informed decisions-making at the right level
- Enhances the legitimacy of a project, especially where some compromise or trade-off is necessary.

A PIA will diagnose what risks, benefits, costs and safeguards are involved.

17. Workplace surveillance

In a number of our work locations, cameras, computers or tracking devices may be used to carry out surveillance of our employees. When this occurs, the Workplace Surveillance Act 2005 must be complied with.

A member of the public is not affected by this, other than perhaps being captured by the video recordings, tracking or other surveillance in place.

In general, an employer may carry out a wide range of surveillance, as long as employees are properly notified. This is called ‘overt surveillance’, or surveillance of which everyone is aware.

Surveillance that employees are not properly notified about is automatically regarded as ‘covert surveillance’ and is generally prohibited by legislation, except for the purpose of establishing whether employees are involved in unlawful activity whilst at work. Covert surveillance can only be done with the authority of a Magistrate.

Recording of private conversations is covered by the Surveillance Devices Act 2007. Legal advice can be sought, internally or externally, by staff, in respect of both workplace surveillance and the recording of private conversations.

If overt surveillance is in place, employees must be given written notice that includes the following items:

1. The kind of surveillance used (e.g. camera, computer, or tracking)
2. How the surveillance will be carried out
3. When it will start
4. Whether it will be continuous or intermittent, and
5. Whether the surveillance will be ongoing or for a specified limited period.

Information or the results collected through overt surveillance, cannot be used or disclosed unless the use or disclosure is:

- Related to the employment of our employees,
- Related to our business activities or functions,

- To a law enforcement agency in relation to an offence,
- Related to civil or criminal proceedings, or
- Reasonably believed necessary to avert an imminent threat of serious violence to persons or substantial damage to property.

A breach of the above restrictions carries a fine. Note that access to the information can be requested by an employee or a person that was captured by the surveillance. Such requests can be made under the PPIPA or the Government Information (Public Access) Act 2009.

18. Breach of privacy/data breach notification

If a data breach is identified, whether serious or not, you will be notified, unless the breach is in relation to information that is not sensitive, poses little to no risk of harm to you, or if it is decided that notification is not required.

A serious data breach is defined as unauthorised access to, unauthorised disclosure of, or loss of, personal information held by us, and as a result, there is a real risk of serious harm to any of the individuals to whom the information relates.

A less serious breach may occur when there is a failure that has caused, or has the potential to cause, unauthorised access to data, such as:

- Accidental loss or theft of classified material data or equipment on which such data is stored (e.g. loss of paper record, laptop, iPad or USB stick)
- Unauthorised use, access to or modification of data or information systems (e.g. sharing of user login details – deliberately or accidentally)
- Compromised user account (e.g. disclosed through phishing)
- Unauthorised disclosure of classified material information (e.g. email sent to incorrect recipient, or posted to incorrect address or addressee, or published on website
- Failed or successful attempts to gain unauthorised access to information
- Equipment failure
- Malware infection
- Disruption to or denial of IT services (where system flooded to break functions).

Data breaches may result in unauthorised collection, use, disclosure or access to personal information. If this happens, we must act quickly to contain the breach, evaluate the risks, consider notifying affected individuals and prevent a repeat.

Notifying individuals can assist in mitigating any damage for those people and reflects positively on our organisation. If the data breach creates a real risk of serious harm to the individual, then they must be notified immediately, or as soon as possible. The Privacy Commissioner should also be notified, if the breach is serious.

A template notification form can be found at Appendix 5.

19. Seeking consent/privacy statement

We are obliged to provide a notification or privacy statement when personal information is collected from you. If your information is to be used for another purpose than what it was collected for, your consent is required to be specifically sought.

Consent means ‘express consent or implied consent’ and should:

- adequately inform you prior to giving consent,
- be provided voluntarily,
- be current and specific, and
- take into account your capacity to understand and communicate your consent.

You can provide express consent either orally or in writing. It may include a handwritten signature, an oral statement, an electronic medium or voice signature.

Implied consent arises where it may be reasonably inferred in the circumstances from your conduct. Silence is not consent. If you do not object to give consent, it does not mean that you have given consent.

Voluntarily should be understood to mean that there was a genuine opportunity for you to provide or withhold your consent. Consent is not voluntary where there is duress, coercion or pressure that could overpower your will.

Opting out is not an advisable way to seek consent. However, there are times when this is our most appropriate option. If an opt-out is used, the following factors, where relevant, must be met:

- The opt out option is clearly and prominently presented
- It is likely the information about collection, use or disclosure and opt-out was read (it formed part of a form filled out by the person, for example)
- Information about the implications of not opting out was given
- The opt-out option is freely available and not bundled with other purposes
- It is easy to choose the opt-out, e.g. little or no cost or effort required to do so
- Consequences of failing to opt-out are not serious
- If opting out later, it will appear as if opted out earlier (as far as practicable).

Bundled consent refers to the practice of putting together multiple requests for your consent to a wide range of collections, uses and disclosure of personal information, without giving you the opportunity to choose which collections, uses and disclosures you agree to and which you do not. It undermines the voluntary nature of the consent and should not be used in a privacy statement or consent request.

Template privacy notifications/ statements can be found at Appendix 6.

20. Promoting the plan

We employ the following broad strategies to ensure ongoing compliance with the privacy legislation:

- As part of our induction program, new staff are provided with information to raise their awareness and appreciation of the privacy legislation requirements
- We provide refresher and on-the-job training for specialist staff
- We highlight and promote the Privacy Management Plan during the annual Privacy Awareness Week/ Month
- Where we propose 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

- We provide specialist advice internally to staff, relating to the interpretation and practical implementation of the privacy legislation
- The Privacy Management Plan is published on our website
- The Privacy Management Plan is reviewed and updated every two years
- Every five years we formally review/ audit our compliance with the privacy legislation. This is due to be undertaken by December 2017.

21. Accountabilities

All staff have a duty to act in accordance with this plan. Staff are also required to comply with the code of conduct and ethical behaviour.

If staff feel uncertain as to whether certain conduct may breach their privacy obligations, they should seek advice from the relevant team in their organisation (see Appendix 4).

21.1 Offences

It is a criminal offence, punishable by up to two years' imprisonment, for any employee (or former employee) of our organisation 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.

Section 308H of the *Crimes Act 1900* provides that it is an offence to access or modify computer records for purposes that are not connected with the duties of the person.

21.2 Protection from liability

Part 8 of the PPIPA and part 8 of the HRIPA also provide certain protections from liability where a person has acted in good faith.

21.3 Responsibilities

Positions with significant responsibilities are:

Position	Responsibility
Secretary/ Chief Executive and Executive	• 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	• 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.
Privacy and Information Access Officers/Staff/ Teams/ Sections in each agency	• 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.

22. Review

We are responsible for reviewing 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 2019.

23. 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, refer to Appendix 4, which lists each relevant agency, our website(s) and contact officer(s).

23.1 Information and Privacy Commission

You can seek advice on the PPIPA, HRIPA from the Office of the Privacy Commissioner:

Phone: 1800 472 679

Email: ipcinfo@ipc.nsw.gov.au

Postal Address - PO Box R232, Royal Exchange NSW 1225

Street Address - Level 5, 47 Bridge Street, Sydney

Website: www.ipc.nsw.gov.au

If you want advice about the *Government Information (Public Access) Act 2009*, you can contact the Office of the Information Commissioner:

Phone: 1800 472 679

Email: ipcinfo@ipc.nsw.gov.au

Postal Address - GPO Box 7011, Sydney NSW 2001

Street Address - Level 17, 201 Elizabeth Street, Sydney

Website: www.ipc.nsw.gov.au

23.2 NSW Civil and Administrative Tribunal (NCAT)

You can lodge an appeal with the NCAT:

Phone: 1300 006 228

Postal address – PO Box K1026, Haymarket NSW 1240

Street Address - Level 10, John Maddison Tower, 86 Goulburn Street, Sydney

Website: http://www.ncat.nsw.gov.au/

A privacy matter would be dealt with by the Administrative and Equal Opportunity Division of the NCAT.

Appendix 1 - Internal review procedures

Any complaint or request for an internal review in relation to a privacy matter is to be forwarded to the relevant privacy officer of the organisation.

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 legal implications or significance of the alleged conduct.

If the application does not meet these criteria it may be referred to relevant managers for handling under relevant complaint handling procedures instead.

A late application may be accepted and the reviewing officer should make a decision about whether to accept it or not. Reasons for not accepting a late application must be communicated to the applicant and the applicant advised how their complaint will be handled instead, as well as their right to complain to the Privacy Commissioner.

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 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, is being conducted
- the reviewing officer's name, title and contact details
- how, or just that, the reviewing officer is independent of the person/s responsible for the alleged conduct (more detail can be provided in the review report)
- 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 the above 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 by this new date (which is likely later than 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 action by way of response or remedy (this may include an apology, changing agency processes, providing training to relevant staff, etc.).

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, taking into consideration any comments or recommendations provided by the Privacy Commissioner, and submit for endorsement by the relevant senior officer (Chief Executive, Secretary, Chief Executive Officer, for example).

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

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

Appendix 2 – Privacy Impact Assessment checklist

If the answer to one or more of the questions below is yes, then a Privacy Impact Assessment should be seriously considered.

Will the project involve?		Yes	No
1	The collection of personal information, compulsorily or otherwise?		
2	A new use of personal information that is already held?		
3	A new or changed system of regular disclosure of personal information, whether to another agency, another State, the private sector, or to the public at large?		
4	Restricting access by individuals to their own personal information?		
5	New or changed confidentiality provisions relating to personal information?		
6	A new or amended requirement to store, secure or retain particular personal information?		
7	A new requirement to sight, collect or use existing ID, such as an individual's driver's licence?		
8	The creation of a new identification system, e.g. using a number, or a biometric?		
9	Linking or matching personal information across or within agencies?		
10	Exchanging or transferring personal information outside NSW?		
11	Handling personal information for research or statistics, de-identified or otherwise?		
12	Powers of entry, search or seize, or other reasons to touch another individual (e.g. taking a blood or saliva sample)?		
13	Surveillance, tracking or monitoring of individuals' movements, behaviour or communications?		
14	Moving or altering premises which include private spaces?		
15	Any other measures that may affect privacy?		

If the above shows a need to carry out a Privacy Impact Assessment, contact the relevant officer of your organisation.

If a PIA is not needed, make a note and copy of the above questions and save to file. This helps if privacy issues arise later in the project and you need to re-visit the list.

A PIA is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals and sets out recommendations for managing, minimising or eliminating that impact.

Even if the list above does not indicate the need for a PIA, it may still be advisable to create a short PIA, particularly if the project will change hands several times. A consistent approach to the management of privacy in the project is crucial.

A PIA should contain some or all of the following 10 steps:

1. Assess the necessity for a PIA – using the above checklist.
2. Plan the PIA – how detailed it needs to be:

- Will it cover one product and service or a group of products and services?
- Identify the primary stakeholders.
- Scope the complexity of the product and service.
- Will there be community or media interest in the outcome?

3. Describe the project (briefly).

- What are the projects overall aims?
- Who is responsible?
- What is the time frame?

4. Identify the stakeholders.

- Who are the stakeholders?
- Are consultations required to discuss potential risks and concerns?

5. Map information flows.

- Map the data life cycle.
- What is collected, how, by whom and here is it going?
- What are the security and quality processes around the data?
- Map the data against compliance with the IPPs and HPPs and identify gaps.

6. Privacy impact analysis and compliance check

- After step 5, analyse the gaps.
- Identify the risks and where they are coming from.
- Identify the data or compliance leakage.

7. Privacy management – addressing risks

- What options will allow you to remove, minimise or mitigate any identified risks?
- Is collection of personal data necessary?
- Are you being transparent enough (privacy notice issued)?

8. Formulate recommendations for future projects.

- Are there any changes that would achieve a more appropriate balance between the project's goals, the interests of affected individuals, and the agency's interests?
- Are any of the identified privacy impacts so significant that the project should not proceed?

9. Prepare the report – to include the following:

- An overall description
- Your PIA method
- Description of the data flows
- Outcome of the PIA and compliance checks
- How to mitigate and avoid future risks
- Identification of the community's response to these risks

10. After the PIA report

- Have you responded to the recommendations in the PIA report?
- Have you engaged an independent review of these recommendations?
- Has the PIA changed due to any changes in the project?

It is not compulsory to have a PIA, but it is recommended.

Appendix 3 – Public Registers

A number of public registers are maintained as required by legislation. Some examples of legislation that requires public registers include (but is not limited to):

- *Contaminated Land Management Act 1997*
- *Dangerous Goods (Road and Rail transport) Act 2008*
- *Environmental Planning and Assessment Act 1979 – (e.g. s.147(12))*
- *Environmental Planning and Assessment Regulation 2000 – (e.g. cl. 25G)*
- *National Parks and Wildlife Act 1974*
- *Protection of the Environment Operations Act*
- *Threatened Species Conservation Act 1995*
- *Wilderness Act 1987*

We also maintain a number of systems:

- Aboriginal Heritage Information Management System (AHIMS)
- Development Assessment System
- Determinations System
- Historic Heritage Information Management Systems (HHIMS).

Public registers can be found on our websites. These are listed at Appendix 4.

Appendix 4 – Contact details

All agencies within the Planning and Environment cluster, as listed below (in alphabetical order), have adopted this plan. This Appendix provides the contact details of the privacy officer as well as relevant functions, legislation and where to locate the public registers.

Centennial Park and Moore Park Trust

Governance Officer

Botanic Gardens & Centennial Parklands

Mrs Macquarie's Road, Sydney NSW 2000

Email: governance.cs@bgcp.nsw.gov.au

The Centennial Park and Moore Park Trust is a statutory body established under the Centennial Park and Moore Park Trust Act 1983. It is responsible for the management and stewardship of Centennial Park

Some of the functions of the Trust include:

- Maintaining and improving Trust lands,
- Consultation with the community, industry and other stakeholders
- Encouraging the use and enjoyment of the Trust lands by the public through recreational, historical, scientific, educational, cultural and environmental events and programs
- Booking out areas of Trust lands for sporting, filming & photography, recreation and events
- Management of licensees, commercial businesses, and activities on Trust lands
- Management of volunteers
- Ensuring the protection of the environment within the Trust lands.

We hold 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 and permits
- event and sports booking applications and plans of management
- complaints and reports from the public
- reports of investigations (e.g. research, audits, ethical conduct, compliance)
- public registers
- public submissions, feedback and comments
- databases of contractors
- financial transactions for payment of goods and services delivered by or to us
- fines issued
- agreements entered into by us with our stakeholders and business partners
- mailing and email distribution lists
- verbal/photographic/audio/video records.

There would also be health and personal records concerning most staff members, such as details about payroll, leave, training, workers compensation, medical certificates and similar/other personnel records.

Department of Planning and Environment (DPE)

Information and Privacy Unit

Department of Planning and Environment

GPO Box 39

SYDNEY NSW 2001

Email: patiunit@planning.nsw.gov.au

Some of the functions of the DPE include:

- consultation with the community, industry and other stakeholders
- registration and recording of development and major project applications
- investigation of complaints, potential breaches of legislation/policies and other allegations
- site audits and inspections
- incident management
- enforcement of environmental and conservation regulations
- issuing licences, approvals, consents and permits
- energy efficiency initiatives with households and businesses
- management of concessions (commercial or business activity) e.g. lease,
- awarding of financial grants
- management of volunteers
- conduct of apprenticeships and other training programs for members of the public
- provision of funding grants
- recommendation or nomination of people or organisations for awards.

We hold 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, development applications and grants
- reports of investigations (e.g. research, audits, ethical conduct, compliance)
- public registers
- public submissions, feedback and comments
- financial transactions for payment of goods and services delivered by or to us
- fines issued
- information agreements and other agreements entered into by us with our 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 publications or email alerts or notifications

- verbal/ photographic/audio/video records.

There would also be health and personal records concerning most staff members, such as details about payroll, leave, training, workers compensation, medical certificates and similar/other personnel records.

Environment Protection Authority (EPA)

Contact a Senior Governance Officer

By telephone: (02) 9995 6080 or 9995 6497

Via email: PIA@environment.nsw.gov.au

By mail: PO Box A290, Sydney South NSW 1232

In person: Level 14 59-61 Goulburn St, Sydney

Website - http://www.environment.nsw.gov.au/whoweare/privacy.htm

The EPA is a statutory corporation established under section 5 of the *Protection of the Environment Administration Act 1991*. The Office of Environment and Heritage (OEH), one of the agencies within the Department of Planning and Environment, has entered into an agreement with the EPA to provide corporate and other essential services.

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.

Some of the functions of the EPA include:

- consultation with the community, industry and other stakeholders
- investigation of complaints, potential breaches of legislation/policies and other allegations
- site audits and inspections
- incident management
- enforcement of environmental and conservation regulations
- issuing licences, approvals, consents and permits
- management of volunteers
- conduct of apprenticeships and other training programs for members of the public
- recommendation or nomination of people or organisations for awards.

We hold 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 and permits
- complaints and reports of environmental and conservation incidents
- reports of investigations (e.g. research, audits, ethical conduct, compliance)
- public registers
- public submissions, feedback and comments
- databases of contractors and site auditors
- financial transactions for payment of goods and services delivered by or to us
- fines issued

- information agreements and other agreements entered into by us with our stakeholders and concession partners
- records of personal achievement for those being nominated for awards
- mailing lists
- subscriptions to publications or email alerts or notifications
- verbal/ photographic/ audio/ video records.

There would also be health and personal records:

- 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.

Our public registers can be found on our website: http://www.epa.nsw.gov.au/publicregister/

Environmental Trust (NSW)

Environmental Trust

Phone: 02 8837 6093

Email: info@environmentaltrust.nsw.gov.au

The NSW Environmental Trust is an independent statutory body established by the NSW government to fund a broad range of organisations to undertake projects that enhance the environment of NSW. The Trust is empowered under the *Environmental Trust Act 1998*, and its main responsibility is to make and supervise the expenditure of grants. The Trust is administered by the Office of Environment and Heritage (OEH) and has adopted the OEH policies and procedures as well as this plan.

The Environmental Trust is chaired by the NSW Minister for the Environment. Members of the Trust are the Chief Executive of OEH, and representatives from local government, the Nature Conservation Council of NSW and NSW Treasury.

Greater Sydney Commission (GSC)

Commissioner Secretary

Greater Sydney Commission

GPO Box 257

Parramatta NSW 2124

info@gsc.nsw.gov.au

Phone: 02 8289 6200

Some of the functions of GSC include:

- provide advice and make recommendations to the Minister on matters relating to planning and development in the Greater Sydney Region
- prepare and provide reports to the Minister on the implementation (including any impediments to the implementation) of any plan or proposal relating to development in the Greater Sydney Region
- provide advice and make recommendations to the Minister on any impediments to the implementation of any plan or proposal relating to development in the Greater Sydney Region

- provide advice to the Minister on the application of any development fund created under section 129 of the Planning Act in respect of land in the Greater Sydney Region
- assist local councils in the Greater Sydney Region and other government agencies (including an agency of the Commonwealth) on the implementation of any plan or proposal relating to development in the Greater Sydney Region
- provide the Minister with such information, advice or reports as the Minister may request
- if requested to do so by a Minister other than the Minister administering this Act (the other Minister), to provide the other Minister with such information, advice or reports as may be requested by the other Minister
- other functions as are conferred or imposed on it by or under GSDC Act or any other Act
- other functions include the power to make local environmental plans under Part 3 of the Planning Act and to prepare draft strategic plans for the Greater Sydney Region under Part 3B of that Act
- exercise functions delegated to it under any other Act.

Hunter Development Corporation

Public Access to Information and Privacy Officer

Hunter Development Corporation

PO Box 813

NEWCASTLE NSW 2300

Email: hdc@hdc.nsw.gov.au

Some of the functions carried out by the Hunter Development Corporation are:

- liaison with the community, industry and other stakeholders
- issuing licences
- management of funding grants
- incident management.

Jenolan Caves Reserve Trust

Trust Administrator (Executive) or General Manager (Senior Manager)

Jenolan Caves Reserve Trust

4655 Jenolan Caves Road

JENOLAN NSW 2790

Phone: 02 6359 3911

Email: reception@jenolancaves.org.au

Website:- http://www.jenolancaves.org.au/about/privacy-policy/

The Jenolan Caves Reserve Trust is a statutory body established under the National Parks and Wildlife Act 1974 Schedule 3 Part 6 Clause 58 and is responsible for the care, control and management of the Jenolan Caves Visitor Use and Services Zone (VUSZ). This Zone contains most of the visitor infrastructure and associated utilities within the Jenolan Karst Conservation Reserve. An Administrator is appointed by the Minister to manage the affairs of the Trust. Approximately 100 (75 FTE) regionally based staff are employed by the Office of Environment and Heritage to assist the Administrator in this role.

The functions of the Trust are similar those applying to the Office of Environment Heritage, but only for the Jenolan VUSZ where the Trust works in collaboration with the National Parks and Wildlife Service, i.e. the park authority responsible for the adjoining Conservation Management Zone within the Reserve.

Joint Regional Planning Panels

Planning Panels Secretariat

320 Pitt Street

Sydney NSW 2000

Email: enquiry@planningpanels.nsw.gov.au

The Planning Panels determine 'regionally significant' development applications (DAs) and certain other Das and modification applications.

Their functions include:

- act as the relevant planning authority (RPA) when directed
- undertake rezoning reviews
- provide advice on other planning and development matters when requested.

Office of Environment and Heritage (OEH)

Contact a Senior Governance Officer

By telephone: (02) 9995 6080 or 9995 6497

Via email: PIA@environment.nsw.gov.au

By mail: PO Box A290, Sydney South NSW 1232

In person: Level 14 59-61 Goulburn St, Sydney

Website - http://www.environment.nsw.gov.au/whoweare/privacy.htm

Some of the functions of the OEH include:

- consultation with the community, industry and other stakeholders
- identification, declaration and management of cultural and heritage sites
- investigation of complaints, potential breaches of legislation/policies and other allegations
- site audits and inspections
- incident management
- enforcement of environmental and conservation regulations
- issuing licences, approvals, consents 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
- awarding of financial grants
- management of volunteers
- conduct of apprenticeships and other training programs for members of the public
- provision of funding grants

- recommendation or nomination of people or organisations for awards.

We hold 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, compliance)
- public registers
- public submissions, feedback and comments
- databases of contractors and site auditors
- financial transactions for payment of goods and services delivered by or to us
- fines issued
- information agreements and other agreements entered into by us with our stakeholders and concession partners
- records of personal achievement for those being nominated for awards
- mailing lists
- Aboriginal site details
- subscriptions to publications or email alerts or notifications
- verbal/ photographic/audio/video records.

There would also be health and personal records:

- relating to the firefighting capability of 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.

Our public registers can be found on our website:
http://www.environment.nsw.gov.au/whoweare/registers.htm

Office of Local Government (OLG)

Office of Local Government

Locked Bag 3015

NOWRA NSW 2541

Email: GIPA@olg.nsw.gov.au

The functions of the OLG include:

- consultation with the community, industry and other stakeholders
- providing advice and information to the State Government and local councils
- regulating financial management and monitoring financial reporting practices of councils
- improving local government performance through provision of standards and guidelines
- conducting reviews and investigations.

Royal Botanic Gardens and Domain Trust

Governance Officer

Botanic Gardens & Centennial Parklands

Mrs Macquaries Road, Sydney NSW 2000

Email: governance.cs@bgcp.nsw.gov.au

The Royal Botanic Gardens and Domain Trust is a statutory body established under the *Royal Botanic Gardens and Domain Trust Act 1980*. It is responsible for the management and stewardship of the Royal Botanic Garden Sydney, the Domain, the Australian Botanic Garden Mount Annan and the Blue Mountains Botanic Garden Mount Tomah.

Some of the functions of the Trust include:

- Maintaining and improving Trust lands as well as the collections of the National Herbarium of New South Wales and the living collection
- To increase and disseminate knowledge about the plant life of Australia, and of New South Wales in particular
- Consultation with the community, industry and other stakeholders
- Encouraging the use and enjoyment of the Trust lands by the public through recreational, historical, scientific, educational, cultural and environmental events and programs
- Booking out areas of Trust lands for sporting, filming & photography, recreation and events
- Management of licensees, commercial businesses, and activities on Trust lands
- Management of volunteers
- Ensuring the protection of the environment within the Trust lands.

We hold 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 and permits
- event and sports booking applications and plans of management
- complaints and reports from the public
- reports of investigations (e.g. research, audits, ethical conduct, compliance)
- public registers
- public submissions, feedback and comments
- databases of contractors
- financial transactions for payment of goods and services delivered by or to us
- fines issued
- Agreements entered into by us with our stakeholders and business partners
- mailing and email distribution lists
- Verbal/ photographic/ audio/ video records.

There would also be health and personal records concerning most staff members, such as details about payroll, leave, training, workers compensation, medical certificates and similar/other personnel records.

Appendix 5 – Breach notification

This Appendix contains a sample breach of privacy notification template that can be used to notify the affected individuals, as well as the Privacy Commissioner, in cases of a privacy breach.

Staff are to modify it to suit the relevant situation and should seek advice from the privacy experts within the agency.

*** SAMPLE ONLY ***

[Use agency letterhead or customise an email to clearly show agency details]

Dear [name]

I am writing to you with important information about a recent data breach involving your personal information / information about your organisation.

We became aware of this breach on [date]. The breach occurred on or about [date] and occurred as follows:

(Describe the event, including, as applicable, the following):

A brief description of what happened.

Description of the data that was inappropriately accessed, collected, used or disclosed.

Steps the individual/organisation should take to protect themselves from potential harm from the breach.

A brief description of what [agency name] is doing to investigate the breach, control or mitigate harm to individuals/organisations and to protect against further breaches.

Please call me with any questions or concerns you may have about the data breach.

[**OPTIONAL -** We have established a section on our website [insert link] with updated information and links to resources that offer information about this data breach.]

We take our role in safeguarding your data and using it in an appropriate manner very seriously. Please be assured that we are doing everything we can to rectify the situation.

Please note that you are entitled to register a complaint with the NSW Privacy Commissioner with regard to this breach.

Should you have any questions regarding this notice or if you would like more information, please contact me by telephone on [number], or via email [email address].

Yours sincerely,

[Name, date and signature blog]

Appendix 6 – Privacy notices and consent

If we do not intend to use or disclose personal or health information, there is no consent required. In all circumstances where we intend to use or disclose personal information, consent from the individual may be required. The Guidance on Consent published by the Office of the Privacy Commissioner of NSW provides useful information on when and how to seek consent.

Following is a template notice to be used by staff whenever personal information is collected and will be used or disclosed by us.

The notice can be amended to suit the relevant purpose and advice can be sought internally from the privacy expert. See Appendix 4 for contact details.

*** SAMPLE ONLY ***

When collecting personal information, we need to inform the person of the following:

- Our contact details,
- Who will hold and/or have access to the information,
- What it will be used for (the purpose of collection),
- What other organisation, if any, routinely (or may) receive this type of information from us (this should include the possibility of the Data Analytics Centre receiving de-identified data),
- Whether the collection is voluntary or required by law,
- Whether we are likely to disclose the information to anyone overseas, and if so, the countries in which the information may be going to (e.g. cloud based information services, overseas provider of services),
- How the person can access and request amendment (if it is inaccurate) of their personal information held by us, and
- If we have obtained the information from someone else, or it is unlikely the person realises we have collected information, what we collect, or have collected, the information, and the circumstances of collection.

As an example, it could be a written notice as follows:

[Name of agency] is requesting this information from you so that we can … [describe the purpose of collection – e.g. providing a service, lodging an application etc.]. We may also … [describe any directly related purpose for which the information might be used – e.g. reporting or program evaluation, publishing summary of submissions]. For the same purpose, [Agency name] may provide this information about you to … [list any persons or organisations that such information is usually disclosed to, outside of the agency – e.g. a contractor or consultant, a service provider etc.].

[**OPTIONAL PARAGRAPH**] When storing your personal information electronically, [agency name] may disclose your personal information to overseas recipients by virtue of its cloud computing arrangements. Our 'cloud' servers are located in [names of countries] and [name of agency] is reasonably satisfied that these countries have similar privacy protections to those afforded under Australian law.

We will not disclose your personal information to anybody else, unless you have given consent, or we are required to do so by law. Our Privacy Management Plan describes when this might occur, particularly sections 8.6 and 10.

Providing us with the requested information is not required by law. If you choose not to provide us with it … [describe the main consequence – e.g. unable to process application or investigate complaint].

You may request access to your information at any time. To access or update your information, or for more details on our privacy obligations, please contact [Name, email and website where privacy management plan can be found].

Secondary purpose consent

To use information for a secondary purpose and when seeking consent for that, the following statement could be used:

*** SAMPLE ONLY ***

With your permission, we would also like to [use/ disclose] your information to … [describe intended secondary purpose – e.g. put on mailing list].

I consent to my personal information being [used/ disclosed] for the purpose of … [name of secondary purpose].

Signature: _____ Date: _____

Name [of person giving consent] _____

Verbal collection of information

When collecting information verbally (e.g. during telephone discussions), we can use less formal wording, so long as we explain how the person's personal information will be used, and to whom we are likely to disclose it to. If the person asks further questions about whether the information is really needed, then we can go into more depth, mention their access and amendment rights and/or offer to let them speak with the Privacy Contact Officer (as listed in Appendix 4).

If we do need to obtain the person's verbal consent to a secondary use or disclosure, we must explain what it is we are asking, and we must ensure that they understand they are free to say 'no'. We must make a file-note of what was said or record it in an appropriate way that can be referred to later, if required.

Appendix 7 – Other privacy related legislation/policies

The key legislation, policies and procedures relevant to privacy 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:

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

Related policies as issued from time to time:

- *Agency Information Guide (GIPA Act)*
- *Code of Ethical Conduct (or similar policy covering ethical behaviour)*
- *Network Acceptable Use Policy (or similar policy)*
- *Public Interest Disclosures Policy and Procedures*

When new policies, procedures and guidelines are devised, we are required to make reference to this plan, to ensure compliance with the PPIPA and the HRIPA. Staff can contact the privacy expert in their agency (see Appendix 4) for assistance and advice.