Privacy Management Plan

Department of Planning, Industry and Environment

November 2020

Published by NSW Department of Planning, Industry and Environment

dpie.nsw.gov.au

Title: Privacy Management Plan

Subtitle: Department of Planning, Industry and Environment

First published: November 2020

This plan should be reviewed every three years.

More information

This has been drafted by the Information Access & Privacy unit, Governance and Legal Group. If you have any questions about this document, please contact the Information Access & Privacy unit on:

T 02 9860 1440
E privacy@dpie.nsw.gov.au

Contents

1. Purpose

The Department of Planning, Industry and Environment (the Department) takes the privacy of our staff and the people of NSW seriously, and we will protect privacy with the use of the Privacy Management Plan as a reference and guidance tool.

The Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act) requires each public sector agency to prepare and implement a Privacy Management Plan (the Plan). Under s33 of the PPIP Act, the Plan must include:

- policies and practices to ensure compliance with the requirements of the PPIP Act or the Health Records and Information Privacy Act 2002 (NSW) (HRIP Act)
- dissemination of those policies and practices to persons within the agency
- internal review procedures
- other matters considered relevant by the agency in relation to privacy and the protection of personal information held by the agency.

2. Introduction

2.1. Summary

This Privacy Management Plan (the Plan) was prepared by the Department and has been made available to all agencies within the Planning, Industry and Environment cluster. The Plan applies to all Departmental staff and the cluster agencies listed in Appendix 1.

The Plan sets out the measures the adopting agencies take to comply with the PPIP Act and the HRIP Act 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 PPIP Act. The Department 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 PPIP Act or the HRIP Act.

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

2.2. Objectives

The PPIP Act and HRIP Act contain principles on how to collect, store, access, amend, use and disclose personal and health information. The PPIP Act 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 health/disability and health/disability services provided to them. There are 15 health privacy principles (HPPs) with which we must also comply.

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 a privacy 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.

2.3. Application and staff responsibilities

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.

All employees, agents, contractors and volunteers are required to comply with the PPIP Act and HRIP Act. Both Acts contain criminal offence provisions applicable to staff, agents and contractors who use or disclose personal information or health information without authority. It is an offence to:

- intentionally disclose or use personal or health information accessed in doing our jobs for an unauthorised purpose
- offer to supply personal or health information for an unauthorised purpose
- attempt by threat, intimidation, etc, to dissuade a person from making or pursuing a request for health information, a complaint to the NSW Privacy Commissioner about health information, or an internal review under the HRIP Act, or
- hinder the Privacy Commissioner or member of staff from doing their job.

It is a criminal offence, punishable by up to two years' imprisonment, an $11,000 fine, or both, for any person employed or engaged by the Department (including former employees and contractors) to intentionally use or disclose any personal information or health information about another person, to which the employee or contractor has or had access in the exercise of his or her official functions, except in connection with the lawful exercise of his or her official functions.

2.4. Definitions

Personal information is defined in section 4 of the PPIP Act 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 PPIP Act 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 HRIP Act 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.

3. Applying the principles

The 12 IPPs are found in sections 8-19 of the PPIP Act, while the 15 HPPs are found in Schedule 1 of the HRIP Act (see Appendix 6). Failure to comply with these principles attract offences under both the PPIP and HRIP Acts.

3.1. Collection of personal information

The collection of information is covered by IPPs 1-4 and HPPs 1-4. We only collect personal information directly from you, where possible. We limit what we collect. For example, we will only ask for your email address if we need to contact you via email.

When we collect information from you, we will explain why it is being collected, what we will use it for, who is likely to receive it, and that you have a right to access and/or modify your personal information.

There may be consequences if you do not provide the personal information requested. For example, we will not be able to contact you if you do not provide an email address or phone number. Where there are consequences to you for failing to provide any requested information, this will also be explained when the information is collected.

Staff members (including contractors and consultants) and volunteers are responsible for meeting these requirements and will usually do so by including a privacy statement or collection notice. This could be on our forms, surveys or questionnaires, in web-based transactions or other instruments.

3.2. Storage of information

IPP 5 and HPP 5 refers to the storage and security of personal information. Each of our business units apply appropriate security to protect personal information. 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. Personal information will be stored, used, retained and disposed of in accordance with the following:

- *State Records Act 1998*
- DPIE Records Management Policy and Advice
- DCS-2020-02 NSW Cyber Security Policy
- Premiers Memorandum M2007-08 Efficient and Cost-Effective Management of Records
- NSW State Records' Standard on records management

3.3. Access and amend your personal information

IPPs 6-8 and HPPs 6-8 provide for access and amendment of your personal information. If you wish to know whether we hold personal information about you, you can contact us directly to enquire. 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.

If you want to access your information, we must grant that access without cost or unreasonable delay. Note that we may require that you prove your identity before granting any request to access or amend your information.

To make an access or amendment request, you should contact the business area holding the information (if known) or contact us at privacy@dpie.nsw.gov.au.

3.4. Using your personal information

IPP and HPP 9 require that we ensure that personal information is accurate, up-to-date, relevant, complete and not misleading before we use it. 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.

IPP and HPP 10 sets the rules for how we use your information. We only use your personal information for the purposes for which it was collected, or a directly related purpose. If there is a need to use the information for another purpose, we would ask for your consent, unless the information is used to prevent an immediate danger to someone's life or health.

There are several exemptions to this provision set out in the PPIP and HRIP Acts. Details of those exemptions are in part 3 of this Plan.

3.5. Disclosing your information

Disclosure of your personal information, that is, providing your information to another agency, organisation or individual, is restricted by IPPs 11 and 12 and HPPs 11 and 14.

We only disclose your information to other parties if:

- you agree to the disclosure or
- you are aware that this sort of information is usually disclosed
- we need to disclose the information to fulfil the purpose for which it was first collected
- information is supplied by us to prevent danger to someone's life or health.

Information about your ethnic or racial origin, political opinions, religious or philosophical beliefs or trade union membership, except to prevent death or injury, is never disclosed without your consent.

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 is authorised or required under legislation. Any exemptions to this are set out in part 3 of this Plan.

3.6. Special provisions for health information

There are some special provisions that only apply to health information contained in HPPs 12, 13 and 15. We may only assign identifiers (e.g. a number) to an individual's health information if it is reasonably necessary for us to carry out our functions. We must not include health information in a health records linkage system without your consent.

People and Culture may collect health information in order to manage cases of injured staff and to investigate workplace incidents. Where health information has been gathered to case manage an injured staff member, it is not given a separate identifier but kept against the relevant employee's

injury management record. Where the information has been gathered as part of an investigation of a workplace incident, the information is held against the investigation file, and not given any separate identifier. People and Culture have no linkages to any health records systems.

4. Other provisions and exemptions

Both the PPIP Act and HRIP Acts specify certain situations when the IPPs and HPPs do not apply.

4.1. Public Registers

A public register is a register of information that is publicly available or open to public inspection. For example, if you own a property, this will be publicly available through a land title information search. Some of your personal information will be publicly available, such as your name, address, and any mortgages or caveats on the property.

Public registers are made under legislation and are exempted from the operation of the IPPs and HPPs by Part 6 of the PPIP Act. If you are concerned about your information being available through a public register, contact the Department.

Some examples of public registers maintained by the Department includes (but is not limited to):

Land Registry Services

- Water access licence register

Environmental Planning and Assessment Act and Regulation

- Political donations and gifts by planning applicants
- Planning agreement register

Biodiversity Conservation Act

- Areas of outstanding biodiversity value
- BioBanking
- Biodiversity conservation programs
- Biodiversity offsets
- Enforceable undertakings
- Kangaroo harvesting licences
- Licences to harm
- Remediation orders
- Threatened species licences
- Wildlife licences

National Parks and Wildlife Act

- Aboriginal heritage impact permits
- Aboriginal Places
- Civil proceedings
- Criminal convictions
- Interim protection orders
- Leases, easements and rights of way
- Remediation directions

Other environmental registers

- Native vegetation public register
- Wilderness protection agreements
- National Parks and Wildlife filming approvals

Crown Lands

- Aboriginal land claims
- Native title claims

4.2. Directions of the Privacy Commissioner

Under section 41 of the PPIP Act and section 62 of the HRIP Act, 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 PPIP Act. Directions currently in operation are listed on the website of the Privacy Commissioner (www.ipc.nsw.gov.au/public-interest-directions).

4.3. Some exemptions in the PPIP ACT or the HRIP ACT

It is worth noting that both the PPIP Act and the HRIP Act provide some specific exemptions from the IPPs and the HPPs.

Some of the exemptions in the PPIP ACT 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).

4.4. 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 Customer Service, or between other government sector agencies. It also provides protections in connection with data sharing and ensures compliance with the requirements of the PPIP Act and HRIP Act 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 business unit. 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.

4.5. Privacy impact assessments (PIA)

A 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.

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 fill out the checklist at Appendix 3. If the answer to one of more of those questions is “yes”, then advice should be sought from the Department’s Information Access and Privacy Unit (Appendix 5) and a PIA should be seriously considered. The IPC can provide guidance on conducting a PIA: https://www.ipc.nsw.gov.au/guide-privacy-impact-assessments-nsw.

5. 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 Plan during Privacy Awareness Week/Month
- We provide specialist privacy advice internally to staff
- The Plan is published on the Department's intranet with links to supporting guidance from the IPC
- The Plan is published on our website and reviewed/updated every two years
- Every five years we formally review and audit our compliance with the privacy legislation.

6. Privacy complaints, breaches and internal reviews

6.1. Privacy 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.

If you want to resolve an issue informally, please contact the relevant area, if known, to discuss your issue. Informal complaints 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 HRIP Act and PPIP Act, complaints or applications for internal review to us must:

- be lodged within six months of becoming aware of the alleged conduct
- be in writing
- have a return address in Australia.

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.

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 there has been a breach of privacy. There is no cost to lodge a complaint or request an internal review. Reviews must be completed within 60 days. The NSW Privacy Commissioner must be advised by the Department of receipt of a privacy internal review request and be provided with the reviewing officer's final report.

The report should:

- detail the review findings about the facts of the matter, the law and the reviewer's interpretation of the law
- set 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 PPIP Act / s.62 of HRIP Act)
    - 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.).

A complaint can also be lodged with the Information and Privacy Commission. (https://www.ipc.nsw.gov.au/)

Detailed internal procedures for handling a privacy internal review are at Appendix 2.

6.2. Breach of privacy/data breach notification

If a data breach is identified, whether serious or not, you will be notified, unless the breach is 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.

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 NSW Privacy Commissioner should also be notified.

If a staff member believes that there has been a breach of privacy, serious or otherwise, they should contact the Department’s Information Access and Privacy Unit as soon as possible (Appendix 5).

Notifications for a privacy breach

Generally, it will be up to the business unit, in consultation with the Information Access and Privacy Unit as needed, to respond to the breach, taking any action to remedy the situation and notifying the affected individuals. A template for notifying any affected individuals is attached at Appendix 4.

A copy of the notification to the affected individuals should be forwarded to the Information Access and Privacy Unit. If it has been decided that the Privacy Commissioner should also be advised, the Information Access and Privacy Unit will then notify the Privacy Commissioner, providing a copy of your notification to the affected individuals.

Appendix 1 – Entities covered by this Plan

The Department has the following Groups:

- Water
- Housing and Property
- Planning and Assessment
- Places, Design and Public Spaces
- Environment, Energy and Science
- Aboriginal Strategy and Outcomes
- Strategy and Reform
- Corporate Services
- People Performance and Culture
- Legal and Governance

There are a number of agencies and statutory authorities which sit within the Departmental cluster and are covered by this Plan, as follows:

- Aboriginal Housing Office
- All National Parks and Wildlife Regional Advisory Committees
- All NSW National Parks
- Biodiversity Conservation Trust
- Boundaries Commission
- Cape Byron Reserve Trust
- Cemeteries Agency (Cemeteries and Crematoria NSW)
- Centennial Parklands and Moore Park Trust
- Cobar Water Board
- Commons Trusts
- Compulsory Acquisition Hardship Review Panel
- Dams Safety NSW
- Dumaresq-Barwon Boards Rivers Commission
- Environmental Trust
- Hartley Historic Site Advisory Committee
- Hay Area - Mawambul Co-management Group
- Hunter and Central Coast Development Corporation
- Karst Management Advisory Committee
- Lands Administration Ministerial Corporation
- Local Government Grants Commission
- Local Government Remuneration Tribunal
- Narran Lakes Reserve Co-management Committee
- National Parks and Wildlife Advisory Council
- National Parks and Wildlife Service Central Coast Hunter Regional Aboriginal Co-management Committee
- Natural Resources Access Regulator
- NSW Coastal Council
- NSW Land and Housing Corporation
- Office of Strategic Lands (Planning Ministerial Corporation)

- Parramatta Parkland Trust
- Place Management NSW
- Property NSW
- Quarantine Station Community Consultative Committee
- Regional Planning Panels Secretariat (Northern, Southern, Western Hunter and Central Coast)
- Royal Botanic Gardens and Domain Trust
- Southern Snowy Mountains Aboriginal Community Executive Advisory Committee
- Sydney District Planning Panels (Eastern City, North, South, Central City, West)
- Sydney Olympic Park Authority
- Teacher Housing Authority of NSW
- Terry Hie Hie Co-Management Committee
- Toorale Joint Management Advisory Committee
- Tubba-Gah Maing Wiradjuri Advisory Committee
- Waste Assets Management Corporation
- Water Administration Ministerial Corporation
- Wollumbin Consultative Group
- Yala Ngurumbang Yindyamarra (Tumut Brungle Gundagai Area Aboriginal Advisory Committee)

Appendix 2 – Privacy internal review procedures

Any complaint or request for an internal review about a privacy matter is to be forwarded to the Information Access and Privacy Unit (see Appendix 5 for contact details).

A senior reviewing officer will be allocated and will:

Step 1 - Assess the application to confirm that:

- it is about personal information regarding conduct that occurred after 1 July 2000, or
- it is about health information regarding 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 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 5 days (see template at attachment 1) of receiving the application stating:

- the officer's understanding of the conduct complained about
- the officer's 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 - Write to the Privacy Commissioner (see template at attachment 2) advising of receipt of the privacy internal review request and providing a copy of your letter to the applicant.

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. The review should use any or all of the following methods:

- review any documentation, such as emails, involved in the alleged conduct
- review any procedures, policies or guidelines that guide the relevant business unit's processes, and what information is provided to members of the public whose personal information is collected
- speak to the officer(s) involved in the alleged conduct
- speak to the applicant to obtain further information

- confer with the director/manager of the area to determine if processes can be amended in order to mitigate future risk of a privacy breach (whether a breach has occurred or not)

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 PPIP Act / s.62 of HRIP Act)
  - 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.

  Note: even if a 'breach' has not occurred, processes can be changed or additional training provided if this would assist to mitigate risk of a breach or the perception of a breach.

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, within 14 days of completing the report (s.53(8) of the PPIP Act):

- 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.

Attachment 1 – template for notification to applicant

Notes for completing this template:

1. the text in green is instructional and should be deleted. Text within square brackets should be amended or deleted as needed.
2. The text below should be pasted into an email, or into a "general letter" template if being sent by post.

Date: [date]
Our Ref:

Dear [Name]

I refer to your request of [date] to the Department of Planning, Industry and Environment (DPIE) for an internal review under section 53 of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) of conduct which led to alleged breaches of the Information Protection Principles (IPPs) under the PPIP Act {and the Health Protection Principles (HPPs) under the *Health Records Information Privacy Act 2002* (HRIP Act)} delete the reference to HRIPA if it is irrelevant.

In your request for a privacy internal review, you state that [brief outline of what is alleged]. You raise concerns that your personal [and health] delete if irrelevant information has not been [stored correctly, has not been protected from unauthorised access, use, disclosure or modification, and that you have been unable to access your personal and health information without excessive delay] amend as necessary.

Relevant Information Protection and Health Privacy Principles

I understand the relevant IPPs and HPPs in this matter to be: Delete those that do not apply

IPP 1 (PPIPA s8) and HPP 1 – Collection: Lawful

An agency must only collect personal information for a lawful purpose. It must be directly related to the agency's function or activities and necessary for that purpose.

IPP 2 (PPIPA s9) and HPP 3 – Collection: Direct

An agency must only collect personal information directly from you, unless you have authorised collection from someone else, or if you are under the age of 16 and the information has been provided by a parent or guardian.

IPP 3 (PPIPA s10) and HPP 4 – Collection: Open

An agency must inform you that the information is being collected, why it is being collected, and who will be storing and using it. You must also be told how you can access and correct your personal information, if the information is required by law or is voluntary, and any consequences that may apply if you decide not to provide it.

IPP 4 (PPIPA s11) and HPP 2 – Collection: Relevant

An agency must ensure that your personal information is relevant, accurate, complete, up-to-date and not excessive. The collection should not unreasonably intrude into your personal affairs.

IPP 5 (PPIPA s12) and HPP 5 – Storage: Secure

An agency must store personal information securely, keep it no longer than necessary and dispose of it appropriately. It should also be protected from unauthorised access, use, modification or disclosure.

IPP 6 (PPIPA s13) and HPP 6 – Transparent

An agency must provide you with details regarding the personal information they are storing, why they are storing it and what rights you have to access it.

IPP 7 (PPIPA s14) and HPP 7 – Accessible

An agency must allow you to access your personal information without excessive delay or expense.

IPP 8 (PPIPA s15) and HPP 8 – Correct

An agency must allow you to update, correct or amend your personal information where necessary.

IPP 9 (PPIPA s16) and HPP 9 – Use: Accurate

An agency must ensure that your personal information is relevant, accurate, up to date and complete before using it.

IPP 10 (PPIPA s17) and HPP 10 – Use: Limited

An agency can only use your personal information for the purpose for which it was collected unless you have given consent, or the use is directly related to a purpose that you would expect, or to prevent or lessen a serious or imminent threat to any person's health or safety.

IPP 11 (PPIPA s18) and HPP 11 – Disclosure: Restricted

An agency can only disclose your information in limited circumstances if you have consented or if you were told at the time they collected it that they would do so. An agency can also disclose your information if it is for a directly related purpose and it can be reasonably assumed that you would not object, if you have been made aware that information of that kind is usually disclosed, or if disclosure is necessary to prevent a serious and imminent threat to any person's health or safety.

IPP 12 (PPIPA s19) – Disclosure: Safeguarded

An agency cannot disclose your sensitive personal information without your consent, for example, information about ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership. It can only disclose sensitive information without consent in order to deal with a serious and imminent threat to any person's health or safety.

HPP 12 – Identifiers

An agency or organisation can only give you an identification number if it is reasonably necessary to carry out their functions efficiently.

HPP 13 – Anonymous

Give the person the option of receiving services from you anonymously, where this is lawful and practicable.

HPP 14 – Transborder transfers

Only transfer health information outside New South Wales in accordance with HPP 14.

HPP 15 – Linkage of health records

Only use health records linkage systems if the person has provided or expressed their consent.

DPIE is conducting a privacy internal review

DPIE is conducting a privacy internal review under section 53 of the PPIP Act [and section 21 of the HRIP Act] delete reference to HRIP Act if irrelevant.

The reviewing officer is myself, [name], [title], Information Access and Privacy Unit. I do not work in [business unit in which alleged conduct took place] and my position does not normally involve [description of the work carried out that is subject to the alleged breach, eg if the complaint is about a social tenancy, say that you do not work within the Land and Housing Corporation and do not normally handle any of their work].

I am therefore performing my role as a reviewing officer independent of the persons responsible for the alleged conduct.

Completion date and review rights

The privacy internal review will be completed **by [60 calendar days]**, which is 60 days from the date your complaint was received by DPIE.

On completion of the review you will be notified within 14 days of:

- the findings of the review
- the actions proposed to be taken by DPIE
- your right to have those findings and proposed actions reviewed by the NSW Civil and Administrative Tribunal (NCAT).

If the review is not completed by [the 60 days date] you are entitled to make an application to NCAT for administrative review of the conduct concerned.

Further information

If you would like to discuss this letter or the progress of the review please contact me on [phone] or via email at [email address].

Regards

Attachment 2 – notification to the Privacy Commissioner template

Notes for completing this template:

1. the text within square brackets should be amended as needed.
2. The text below should be pasted into an email and sent to info@ipc.nsw.gov.au. Make sure to attach a copy of your notification to the applicant.

Dear IPC

Please be advised that the Department of Planning, Industry and Environment received a request for a privacy internal review under section 53 of the *Privacy and Personal Information Protection Act 1998* on [date] from [applicant].

I have attached a copy of her/his application. Attached also is our acknowledgement of her/his application, notifying of the investigating officer (myself) and the due date for completion of the investigation.

Please do not hesitate to contact me if you have any queries about this matter.

Regards

Appendix 3 – Privacy impact assessment checklist

Table – Checklist for whether a Privacy Impact Assessment is needed

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?		

Appendix 4 – Data Breach notification template

Notes for completing this template:

1. the text in green is instructional and should be deleted. Text within square brackets should be amended or deleted as needed.
2. The text below should be pasted into an email, or into a “general letter” template if being sent by post.

Our ref:

Dear [name]

I am writing to inform you a breach of your privacy on [date] by [business division], a division of the Department of Planning, Industry and Environment (DPIE), regarding [brief description of what aspect of their information has been breached, eg “your land tax online account”].

On behalf of DPIE, I apologise for this breach, and any concern this may raise with you.

This occurred when [describe how the breach occurred].

[Describe what information was disclosed].

[Describe what DPIE has done to mitigate any future breach].

DPIE takes privacy seriously. You can find out more about our privacy policies on our website (https://www.planning.nsw.gov.au/Privacy). Information about [business division, if they have their own website] and privacy can also be found on the [business division website address] delete this sentence if your business area does not have its own website. I have enclosed a fact sheet from the Information and Privacy Commission (IPC) about privacy laws in NSW. Further information about your rights, as well as how to lodge a privacy internal review, is available from the IPC (www.ipc.nsw.gov.au). [Note: this fact sheet is also available in other languages and an appropriate fact sheet should be sent if available: https://www.ipc.nsw.gov.au/guide-privacy-laws-nsw.]

If you have any questions or would like further information, please contact me on [phone] or by email at [email address].

Regards

Appendix 5 – Contacts

For assistance with privacy issues

DPIE Information Access and Privacy unit

Email: privacy@dpie.nsw.gov.au
Phone: 02 9860 1440
Post: 4 Parramatta Square, Locked Bag 5022, Parramatta NSW 2124

Information and Privacy Commission

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

NSW Civil and Administrative Tribunal

Administrative and Equal Opportunity Division and Occupational Division

Email: aeod@ncat.nsw.gov.au
Phone: 1300 006 228 and press 3 for the Administrative and Equal Opportunity and Occupational Divisions
Post: PO Box K1026, Haymarket NSW 1240 | DX 11539 Sydney Downtown
Street: Level 10 John Maddison Tower, 86-90 Goulburn Street Sydney

Contacts for other agencies not covered by this plan:

Department of Regional NSW

Email: gipa@regional.nsw.gov.au
Phone: 0438 466 024
Post: 4 Parramatta Square, Locked Bag 5022, Parramatta NSW 2124

Environmental Protection Authority (EPA)

Email: gipa.privacy@epa.nsw.gov.au
Phone: 02 9995 6497 or 02 9995 6099
Post: 4 Parramatta Square, Locked Bag 5022, Parramatta NSW 2124

Independent Planning Commission of NSW

Email: ipcn@ipcn.nsw.gov.au
Phone: (02) 9383 2100
Post: Level 3, 201 Elizabeth Street, Sydney, NSW 2000

Natural Resources Commission

Email: nrc@nrc.nsw.gov.au
Phone: 02 9228 4844
Post: GPO Box 5341, Sydney NSW 2001

Appendix 6 – Protection Principles

The Information Protection Principles (IPPs)

Explained for members of the public (IPC Fact sheet, August 2019)

The 12 Information Protection Principles (IPPs) are your key to the *Privacy and Personal Information Protection Act 1998* (PPIP Act)

These are legal obligations which NSW public sector agencies, statutory bodies, universities and local councils must abide by when they collect, store, use or disclose personal information.

As exemptions may apply in some instances, it is therefore suggested you contact the Privacy Contact Officer at the agency or the Information and Privacy Commission NSW (IPC) for further advice.

Collection

1. Lawful

An agency must only collect personal information for a lawful purpose. It must be directly related to the agency's function or activities and necessary for that purpose.

2. Direct

An agency must only collect personal information directly from you, unless you have authorised collection from someone else, or if you are under the age of 16 and the information has been provided by a parent or guardian.

3. Open

An agency must inform you that the information is being collected, why it is being collected, and who will be storing and using it. You must also be told how you can access and correct your personal information, if the information is required by law or is voluntary, and any consequences that may apply if you decide not to provide it.

4. Relevant

An agency must ensure that your personal information is relevant, accurate, complete, up-to-date and not excessive. The collection should not unreasonably intrude into your personal affairs.

Storage

5. Secure

An agency must store personal information securely, keep it no longer than necessary and dispose of it appropriately. It should also be protected from unauthorised access, use, modification or disclosure.

Access and accuracy

6. Transparent

An agency must provide you with details regarding the personal information they are storing, why they are storing it and what rights you have to access it.

7. Accessible

An agency must allow you to access your personal information without excessive delay or expense.

8. Correct

An agency must allow you to update, correct or amend your personal information where necessary.

Use

9. Accurate

An agency must ensure that your personal information is relevant, accurate, up to date and complete before using it.

10. Limited

An agency can only use your personal information for the purpose for which it was collected unless you have given consent, or the use is directly related to a purpose that you would expect, or to prevent or lessen a serious or imminent threat to any person's health or safety.

Disclosure

11. Restricted

An agency can only disclose your information in limited circumstances if you have consented or if you were told at the time they collected it that they would do so. An agency can also disclose your information if it is for a directly related purpose and it can be reasonably assumed that you would not object, if you have been made aware that information of that kind is usually disclosed, or if disclosure is necessary to prevent a serious and imminent threat to any person's health or safety.

12. Safeguarded

An agency cannot disclose your sensitive personal information without your consent, for example, information about ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership. It can only disclose sensitive information without consent in order to deal with a serious and imminent threat to any person's health or safety.

The Health Privacy Principles (HPPs)

Explained for members of the public (IPC Fact Sheet, August 2019)

The 15 Health Privacy Principles (HPPs) are the key to the *Health Records and Information Privacy Act 2002* (HRIP Act).

These are legal obligations which NSW public sector agencies and private sector organisations must abide by when they collect, hold, use and disclose a person's health information. Exemptions may apply, therefore it is suggested you contact the Privacy Contact Officer or the Health Information Manager in the organisation or agency in the first instance. Or contact the Information and Privacy Commission NSW (IPC) for further advice.

Collection

1. Lawful

An agency or organisation can only collect your health information for a lawful purpose. It must also be directly related to the agency or organisation's activities and necessary for that purpose.

2. Relevant

An agency or organisation must ensure that your health information is relevant, accurate, up-to-date and not excessive. The collection should not unreasonably intrude into your personal affairs.

3. Direct

An agency or organisation must collect your health information directly from you, unless it is unreasonable or impracticable to do so.

4. Open

An agency or organisation must inform you of why your health information is being collected, what will be done with it and who else might access it. You must also be told how you can access and correct your health information, and any consequences if you decide not to provide it.

Storage

5. Secure

An agency or organisation must store your personal information securely, keep it no longer than necessary and dispose of it appropriately. It should also be protected from unauthorised access, use or disclosure.

Access and accuracy

6. Transparent

An agency or organisation must provide you with details regarding the health information they are storing, why they are storing it and what rights you have to access it.

7. Accessible

An agency or organisation must allow you to access your health information without unreasonable delay or expense.

8. Correct

Allows a person to update, correct or amend their personal information where necessary.

9. Accurate

Ensures that the health information is relevant and accurate before being used.

Use

10. Limited

An agency or organisation can only use your health information for the purpose for which it was collected or a directly related purpose that you would expect (unless one of the exemptions in HPP 10 applies). Otherwise separate consent is required.

Disclosure

11. Limited

An agency or organisation can only disclose your health information for the purpose for which it was collected or a directly related purpose that you would expect (unless one of the exemptions in HPP 11 applies). Otherwise separate consent is required.

Identifiers and anonymity

12. Not identified

An agency or organisation can only give you an identification number if it is reasonably necessary to carry out their functions efficiently.

13. Anonymous

Give the person the option of receiving services from you anonymously, where this is lawful and practicable.

Transferrals and linkage

14. Controlled

Only transfer health information outside New South Wales in accordance with HPP 14.

15. Authorised

Only use health records linkage systems if the person has provided or expressed their consent.