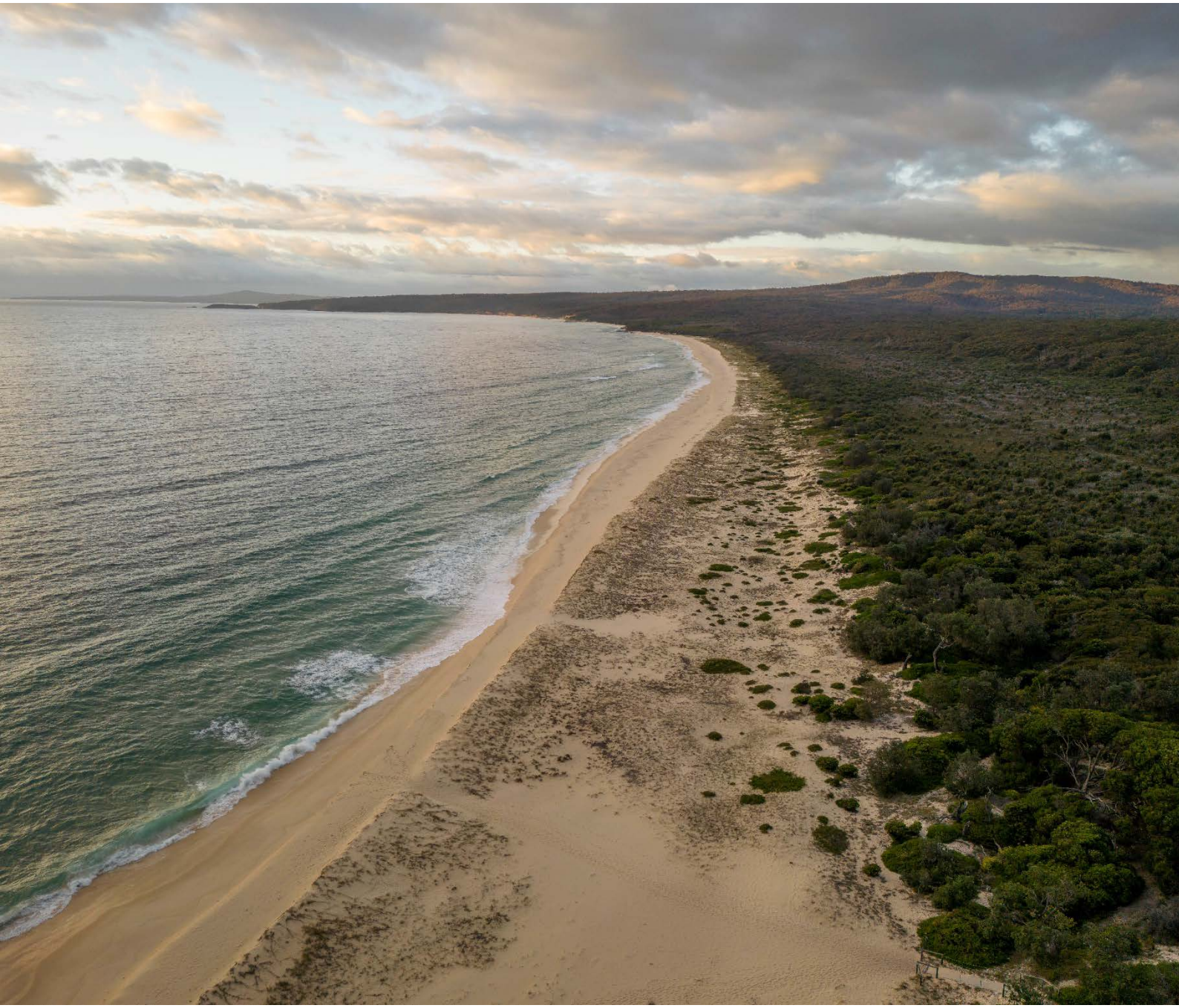

Privacy Management Plan

**Department of Climate Change,
Energy, the Environment and Water**

NSW GOVERNMENT

Acknowledgement of Country

Department of Climate Change, Energy, the Environment and Water acknowledges the Traditional Custodians of the lands where we work and live.

We pay our respects to Elders past, present and emerging.

This resource may contain images or names of deceased persons in photographs or historical content.

Cover photo: Haycock Point, Beowa National Park John Spencer/DCCEEW

Published by:

Department of Climate Change,
Energy, the Environment and Water
Locked Bag 5022, Parramatta NSW 2124
Phone: +61 2 9995 5000 (switchboard)
TTY users: phone 133 677, then ask for 1300 361 967
Speak and listen users: phone 1300 555 727, then ask for 1300 361 967
Website nsw.gov.au/dcceew

May 2024

Find out more at:

dcceew.nsw.gov.au

Contents

List of tables

Purpose

The Department of Climate Change, Energy, the Environment and Water (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) (the 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) (the HRIP Act)
- dissemination of those policies and practices to persons within the agency
- internal review procedures
- other matters considered relevant by the agency to privacy and the protection of personal information held by the agency.

Introduction

Summary

This Plan was prepared by the Department and has been made available to all agencies within the Climate Change, Energy. the Environment and Water (the Department) network of agencies. The Plan applies to all Departmental staff and the agencies listed in Appendix 1.

Some of the business areas and agencies with the Department network maintain their own branded websites. Where applicable, a privacy policy with more detailed references to the specific information handled by that area of the Department will be available on the relevant website. This Plan should be read in conjunction with any such online privacy statement.

Service NSW provides services to some customers of the Department on our behalf, including the National Parks and Wildlife Service and the Energy Social Programs. This Plan applies whether services are provided directly by the Department or by Service NSW. For more information about Service NSW visit www.service.nsw.gov.au.

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.

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, privacy (data) breach response, 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.

Application and staff responsibilities

This plan applies to all staff engaged by us, whether by permanent (ongoing) appointment, 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 2 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.

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.

Business area / unit are branches, divisions and groups within the Department which specialise and handle specific types of work. For example, the Water Infrastructure division deals with the building of dams and other infrastructure on NSW waterways. You can see a full list of all the business areas within the Department here.

Network agencies are statutory entities that sit within the Department of Climate Change, Energy, the Environment and Water and have adopted this plan (see Appendix 1).

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. Failure to comply with these principles attract offences under both the PPIP and HRIP Acts.

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 to what is necessary, and only for a lawful purpose. 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.

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
- DPE 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

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.

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 may also be specific other uses outlined in privacy collection statements for specific transactions you undertake with us. For example, if you have engaged with us for a particular program, we will advise that we may use your information to evaluate and review the program in question.

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

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 one of the following applies:

- you agree to the disclosure
- 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 unless:

- you agree to the disclosure
- the disclosure is necessary for an investigative function
- information is supplied by us to prevent danger to someone's life or health.

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.

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.

The People and Culture branch 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.

Other provisions and exemptions

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

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. Part 6 of the PPIP Act requires that an agency be mindful of the IPPs and HPPs when publishing a public register, but some personal information may still be made public if the purpose of the register requires it. For example, the register for gifts and benefits offered to public sector staff must include the name of the person offering the benefit.

If you are concerned about your information being available through a public register, you can request suppression of your information by contacting the Department.

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

Water

- Water access licence 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

Governance

- Gifts, Benefits & Hospitality register

Directions of the Privacy Commissioner and codes of practice

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 of the application of an IPP or HPP is needed, then a Code of Practice may be more appropriate.

Part 3 of the PPIP Act and Part 5 of the HRIP Act provide for the making of a privacy Code of Practice. Any such Code is reviewed by the Privacy Commissioner and approved by the Minister. A Code can regulate an agency's collection, storage, use or disclosure of personal information, or modify the operation of the IPPs and HPPs when applied in specific circumstances.

Directions and Codes of Practice currently in operation are listed on the website of the Privacy Commissioner (www.ipc.nsw.gov.au/public-interest-directions and www.ipc.nsw.gov.au/privacy-codes-practice).

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 for ICAC, NSW Police Force, Police Integrity Commission, and the NSW Crime Commission (section 27)
- certain exchanges between public sector agencies (section 27A)
- research (section 27B)
- credit information (section 27C)
- other exemptions (section 28).

Data Analytics Centre and sharing information with other agencies

The *Data Sharing (Government Sector) Act 2015* (DSGS Act) was created to promote sharing of information for certain purposes. This includes 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 or another government agency to provide information, we consult internally with the relevant subject matter experts. 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. Options considered before deciding whether to share requested information includes:

- Can the information be de-identified before sharing?
- Can aggregated data be used instead?
- What safeguards are in place to ensure secure transfer, storage and access to the data?

When sharing data, we will usually put strong agreements in place so the receiving agency is clear on the sensitivity of the data and the need to limit the use of the data to the project it is specifically shared for.

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.

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 or 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 Department uses the Privacy Risk Procedure, adapted from materials from Salinger Privacy©, to determine whether a PIA is needed.

If a PIA is needed, the Department may undertake the assessment internally or engage an external consultant. The level of risk and the size of the project will help determine which option is best. The Department also takes into consideration the guidance provided by the IPC on conducting a PIA.:

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
- We provide specialist privacy advice internally to staff
- The Plan is linked from the Department's intranet with links to supporting guidance from the IPC
- The Plan is published on our website and reviewed/updated at least every 1-2 years
- Every 5 years we formally review and audit our compliance with the privacy legislation.

Privacy complaints, breaches and internal reviews

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.

Informal complaint

If you make an informal complaint, our Information Access & Privacy unit will work with the relevant business area in the Department to correct any problems, such as removing information that has been inappropriately published, and to contain any potential harm caused. We might also work to improve processes and procedures to minimise the risk of similar problems happening again. We will let you know the outcome of any actions we take.

See the Breach of privacy/data breach chapter below for more information on how we handle privacy breaches.

If you want to resolve an issue informally, please contact the relevant area of the Department, if known, to discuss your issue. You can also contact the Department's Information Access & Privacy unit at privacy.dcceew@environment.nsw.gov.au.

Formal complaint – privacy internal review

Informal complaints may be referred for a review to be carried out under section 53 of the PPIP Act, 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. You can also ask for a review to be carried out. This is known as a privacy internal review.

Under the HRIP Act and PPIP Act, complaints or applications for internal review to us must:

- be lodged within 6 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 that led to the potential privacy breach, and deciding if there has been a breach of privacy. There is no cost to lodge a complaint or request an internal review. Reviews should 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.

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

Breach of privacy/data breach

We might become aware of a breach of privacy either because you make a complaint about your privacy being breached, or a Departmental employee identifies that something has happened that may have exposed a person's privacy. In either circumstance, the matter will be forwarded to our Information Access & Privacy unit. The business area responsible for the conduct that led to the breach will do their best to contain the breach and minimise any damage to you or others affected.

The Information Access & Privacy unit will assist the business area responsible, assess the seriousness of the breach, and make any recommendations such as:

- notification to any affected individuals
- notification to the NSW Privacy Commissioner
- changes to processes or procedures that would minimise the risk of a future breach.

If a serious data breach is identified, you will be notified in accordance with the mandatory data breach notification scheme. The Department will also notify you if the breach is not serious, 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.

Procedures for handling eligible data breaches are at Appendix 4.

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, they must be notified immediately, or as soon as possible. The NSW Privacy Commissioner must also be notified. The Department might also notify the Privacy Commissioner if the risk is not serious, but we believe it is best to do so.

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

Mandatory data breach notification scheme

As of 28 November 2023, all NSW government agencies are required to comply with the mandatory data breach notification scheme. You can view the Department's Privacy (data) breach policy on our website here. Our procedures for responding to an eligible data breach are at Appendix 4.

Notifications for a privacy breach

Generally, it will be up to the business unit responsible for the conduct that led to the breach, in consultation with the Information Access and Privacy Unit as needed, to respond to the situation, taking any action to remedy the matter and notifying the affected individuals.

If Department staff receive a complaint alleging a privacy breach, or identify for themselves that a breach of privacy may have occurred, they should contact the Information Access and Privacy Unit as soon as possible. The Unit can guide the business area in handling the matter, such as suggesting remedies and assisting with notifications to affected individuals. The Unit will also help to assess whether the breach meets the threshold serious enough to require notification to the NSW Privacy Commissioner.

A copy of any notification to the affected individuals should be forwarded to the Information Access and Privacy Unit. If the matter has been assessed as likely to result in serious harm to an individual, the Information Access and Privacy Unit will then notify the Privacy Commissioner, providing a copy of the Department's notification to the affected individuals. The Information Access and Privacy Unit will be the Department's liaison with the Privacy Commissioner and assist the business area in assessing and responding to any recommendations of the Commissioner.

The Information Access and Privacy Unit maintains a register of all possible breaches, including complaints, whether or not an assessment finds that a breach did occur. The Unit takes the lead on reporting on breaches to the Department's senior leadership team, as needed. The Unit is also responsible for providing the statistical information for the Department's annual reporting requirements.

Appendix 1 – Entities covered by this Plan

The Department has the following Groups:

- Corporate Services
- Energy Corporation of NSW (EnergyCo NSW)
- National Parks and Wildlife Services
- Biodiversity, Conservation and Science
- Heritage
- Energy, Climate Change & Sustainability
- Water

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

- Biodiversity Conservation Trust (in conjunction with their privacy management plan)
- Dams Safety NSW
- Dumaresq-Barwon Boards Rivers Commission
- Environmental Trust
- Hartley Historic Site Advisory Committee
- Hay Area - Mawambul Co-management Group
- Heritage Council of NSW
- Jenolan Caves Reserve Trust
- Karst Management Advisory Committee
- Lord Howe Island Board
- Narran Lakes Reserve Co-management Committee
- National Parks and Wildlife Advisory Council
- National Parks and Wildlife Regional Advisory Committees (all)
- National Parks and Wildlife Service Central Coast Hunter Regional Aboriginal Co-management Committee
- Natural Resources Access Regulator (in conjunction with their privacy management plan)
- NSW Coastal Council
- Quarantine Station Community Consultative Committee
- Southern Snowy Mountains Aboriginal Community Executive Advisory Committee
- Terry Hie Hie Co-Management Committee
- Toorale Joint Management Advisory Committee
- Tubba-Gah Maing Wiradjuri Advisory Committee
- Water Administration Ministerial Corporation
- Wollumbin Consultative Group

- Yala Ngurumbang Yindyamarra (Tumut Brungle Gundagai Area Aboriginal Advisory Committee)

Appendix 2 – Privacy internal review procedures

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

A senior officer within the unit will be allocated as the reviewing officer and will carry out the following steps.

Step 1 Assess the application to confirm that:

- it has been lodged within 6 months of the individual becoming aware of the alleged conduct, and
- it is about either:
  - personal information and conduct that occurred after 1 July 2000, or
  - health information and conduct that occurred after 1 September 2004

If the above criteria are not met, the matter may be referred to relevant manager(s) for handling under other relevant complaint handling procedures instead.

If the criteria are met, the reviewing officer will proceed with the next steps.

Late applications

Applications may be accepted outside of the required 6-month period. The reviewing officer should consider the specific circumstances to the case and make a decision about whether there are sufficient grounds to accept a late application. The reviewing officer may need to engage with the relevant business area in making this decision.

1. If the late application is accepted, this will be communicated to the business area and the officer will proceed with the next steps.
2. If it is not accepted, the reasons for the decision must be communicated to the complainant. The complainant is to be advised of any next steps the Department intends to take (if any), and their right to complain to the NSW Privacy Commissioner.

Step 2 Engage with the relevant business area of the Department to advise:

- that the application has been received, and
- of the process, the next steps and what their requirements will be.

The reviewing officer will notify the business area of the matter. The business area must nominate a person who is sufficiently senior to be able to approve any process changes, should the review make recommendations for it.

The business area must also ensure that someone who has sufficient subject matter expertise is available to respond promptly to queries from the reviewing officer.

Step 3 Write to the complainant within 5 days of receiving the application stating:

- the officer's understanding of the conduct complained about
- the officer's understanding of the relevant 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 business area and was not substantially involved in any matter in connection with the conduct complained about
- a date 60 days from the day the application was received and a statement that if the review is not completed within the 60 days, the complainant 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, and
- that a copy of the letter will be provided to the Privacy Commissioner who has an oversight role.

Step 4 Write to the Privacy Commissioner to advise of the privacy internal review request and provide a copy of the letter to the complainant (see Step 3).

Step 5 Gather information and review the evidence to determine whether the alleged conduct occurred, and if so, whether it constituted a 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 complainant to obtain further information and find out what it is they are seeking to manage their expectations about what we can and can't do
- confer with a director or manager of any relevant business 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 6 Send a progress report if the review is not finalised within 4 weeks of the issuing of the letters at steps 2 and 3 above to the complainant, with the Privacy Commissioner copied in, detailing:

- the progress to date, and where appropriate, the next steps
- any anticipated delays, and
- a reminder that if the review is not completed by the due date, the complainant can go to NCAT for an external review of the alleged conduct.

Step 7 Write a draft report after the review is completed:

- detailing the review findings, the relevant privacy law and how it applies to the facts of the matter
- for each information protection principle, setting out a determination as to whether a breach has occurred, with one of the following findings:
  - there is insufficient evidence to demonstrate the alleged conduct occurred
  - the alleged conduct occurred but it was in compliance with the relevant privacy/health privacy principles and/or public register provisions
  - the alleged conduct occurred, but non-compliance was allowed under a specified exemption, Code or Direction (s.41 of PPIP Act / s.62 of HRIP Act), or
  - the alleged conducted occurred and it did not comply with principles or public register provisions, so constitutes a 'breach', and
- where appropriate, making recommendations or remedy that may include a formal apology, a change to processes, providing training to staff, or monetary compensation to the complainant.

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 future breach or the perception that a future breach is likely to occur.

Step 8 Liaise with the business area to provide a copy of the findings and recommendations. The business area should review the findings and advise the reviewing officer whether the recommendations are:

- agreed to, practical, and able to be implemented, or
- onerous or expensive, and not agreed to.

A sufficiently senior person within the business area should approve any recommended changes to processes or procedures and ensure they are implemented.

If the recommendations are impractical, unreasonably onerous, or expensive, the business area must work with the reviewing officer to find a course of action that will serve to mitigate future risks and comply with the Department's obligations under the PPIP Act.

Note: even if recommendations are onerous or expensive, any decision about whether to accept the recommendations should have mind of the Department's obligations under the PPIP Act and future liability if further breaches of privacy occur as a result of failing to take action.

Step 9 Provide a copy of the draft report to the Privacy Commissioner for comment, and check whether the Commissioner wishes to make any submissions.

Step 10 Finalise the report, taking into consideration any comments or recommendations provided by the Privacy Commissioner.

Step 11 Notify the business area, complainant and the Privacy Commissioner in writing and within 14 days (s.53(8) of the PPIP Act):

- that the review is finished
- of the review findings, including the reasons and legislative basis for the findings, and any action proposed to be taken, and
- of the complainant's right to apply within 28 days to the NSW Civil and Administrative Tribunal (NCAT) for a further review, and the details for the NCAT.

Contact

Information Access & Privacy unit

Ph: 02 9860 1440

Email: privacy.dcceew@environment.nsw.gov.au

Appendix 3 – Privacy impact assessment checklist

Table 1 - Checklist for whether a Privacy Impact Assessment is needed

	What 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 – Privacy (Data) Breach procedures – quick guide

Note: this is a quick guide only. The detailed procedure manual for handling privacy breaches and complaints is maintained by the Information Access and Privacy team.

Table 2 – Privacy (Data) breach procedures - quick guide

Role	Responsibility
As soon as a breach is identified, it must be reported to the Information Access and Privacy unit.	All staff
Take immediate steps to contain the breach and mitigate any harm. This might include contacting incorrect recipients of emails and requesting that emails be deleted or taking action to remove content from social media or a website. Where a privacy breach is also a potential cyber incident, the Chief Information Security Officer must be advised as soon as possible.	Relevant business area responsible for the action that led to the breach (or suspected breach). The Information Access and Privacy team will assist the business area.
The Secretary's delegate will appoint an assessor to review the breach and determine whether it's likely to be an eligible data breach.	Delegates: • General Counsel, or • Chief Operating Officer The Information Access and Privacy team will usually be either the appointed assessor or support the appointed assessor.
If the assessment cannot be completed with 30 days, an extension of assessment period can be approved by the Secretary's delegate, if it is necessary.	• General Counsel, or • Chief Operating Officer
The Secretary 's delegate will make a decision as to whether the breach is an eligible data breach.	• General Counsel, or • Chief Operating Officer
Notifications of eligible data breaches to the Privacy Commissioner.	The Information Access & Privacy team

Role	Responsibility
Notification to affected individuals – this is mandatory if the matter has been assessed as an eligible data breach. The Department also voluntarily notifies affected individuals unless the risk to them is minor.	Director-level or above in the business area responsible for the breach will notify any affected individuals – the Information Access & Privacy team can provide support.
The Secretary's delegate will approve a notice to be published if any of the affected individuals cannot be notified, or it is not practicable to notify all individuals.	• General Counsel, or • Chief Operating Officer The Information Access and Privacy team will support this process and maintain the public register.
The agency should consider any support we could provide to affected individuals. Depending on the type of harm, individuals can be referred to: • counselling services • IDCare – supports victims of identity theft and cyber security breaches • cyber.gov.au – Australian Government agency that helps people to recover from cyber threats • ID Support NSW – NSW Government agency that helps people with loss of identity documents • another agency (including police) that is in a position to take action to assist the person the Employee Assistance Program (EAP) – if the affected individual is a staff member.	The business area responsible for the breach and the Information Access & Privacy team should make any referrals at the time of dealing with affected individuals.
The Secretary's delegate may decide, in limited circumstances, that an exemption from requirements for notifying individuals of an eligible data breach may apply. There are several exemption types, for example when notification would breach secrecy provisions. The assessment of the breach will determine if an exemption applies.	• General Counsel, or • Chief Operating Officer

The Department's workflow for handling privacy (data) breaches can be found on the next page.

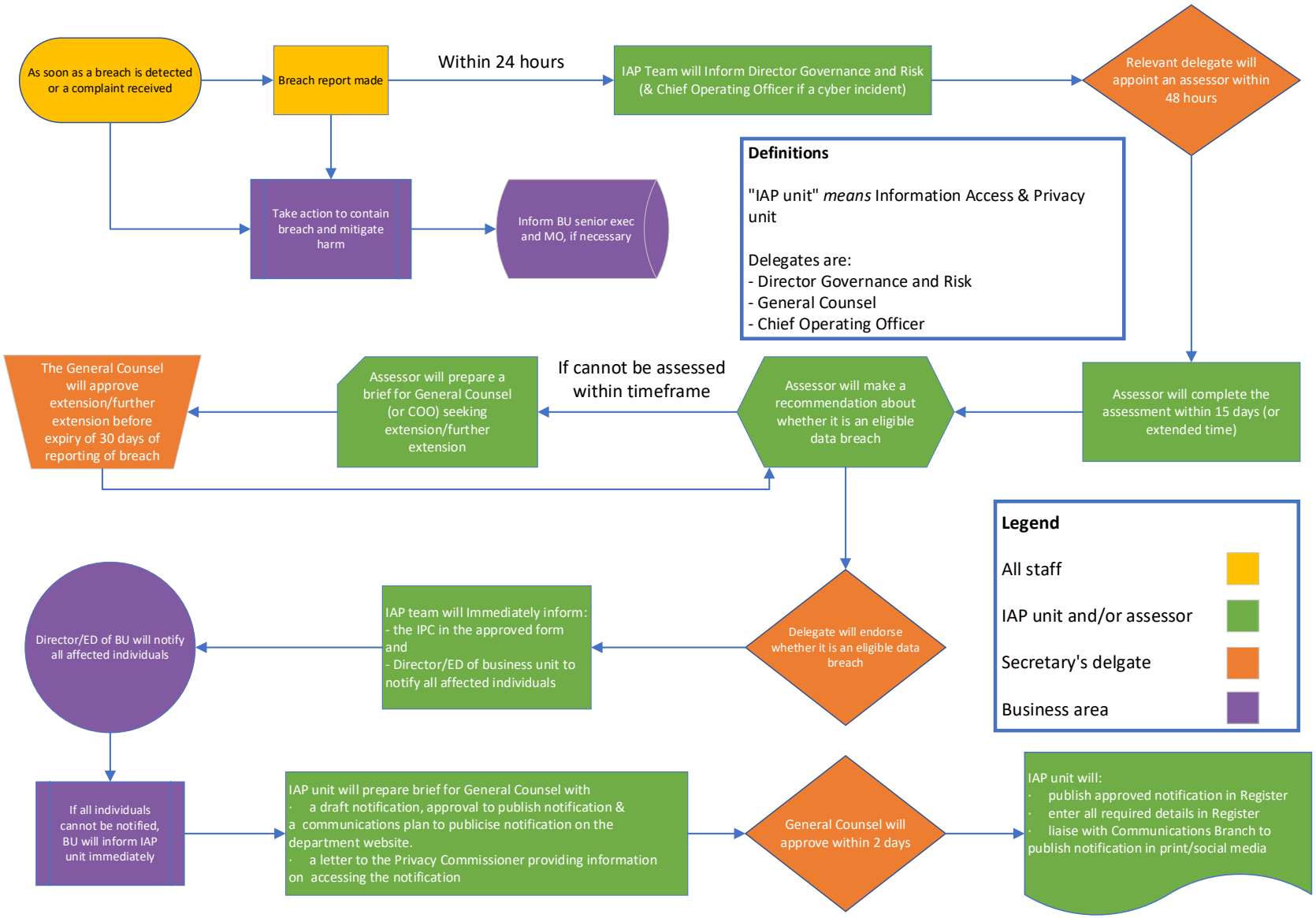

Figure 1 - Privacy breach workflow

Appendix 5 – Contacts

For assistance with privacy issues

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: ipcinfo@ipc.nsw.gov.au

Phone: 1800 472 679

Address: Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000

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

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

Table 3 - Document control

Document version history	
First Published	March 2024
Due to review	March 2026
Document version number	1
Document reference number	DOC24/212679