Privacy (Data) Breach Policy

Purpose of this policy

The purpose of this policy is to set out the requirements for mandatory notification of certain privacy breaches.

Under the *Privacy and Personal Information Protection Act 1998* (PPIP Act), the Department of Planning and Environment (the department) is required to ensure that the personal and health information that it holds is kept safe from unauthorised access, use, disclosure or loss.

If personal or health information is used or disclosed without authority, the department is required to take action to contain the breach and mitigate any harm. The department is also required to notify affected individuals and the Privacy Commissioner of an eligible data breach.

To whom this policy applies

This policy applies to all employees, volunteers, consultants, and contractors of the department and of portfolio agencies that are included in the department's Privacy Management Plan.

Policy statement

Everyone covered by this policy is required to report all known and suspected breaches, regardless of how serious or minor. The department takes a precautionary approach, and all breaches are assessed to ensure we fulfill our reporting and notification obligations. Early reporting helps the department contain a breach and mitigate harm.

What is an 'eligible data breach'?

An eligible breach occurs when personal or health information held by an agency is subject to:

- unauthorised access;
- unauthorised disclosure; or
- is lost in circumstances where the loss is likely to result in unauthorised access or unauthorised disclosure,

and where the access, disclosure or loss is likely to cause serious harm to the person to whom the information relates.

An eligible data breach can still occur even if the disclosure is within the department.

SF23/60759

What is 'serious harm'?

Harm to an individual includes:

- physical harm
- economic, financial or material harm
- emotional or psychological harm
- reputational harm; and
- other forms of serious harm that a reasonable person in the agency's position would identify as a possible outcome of the data breach.

Whether a particular data breach would be considered likely to cause serious harm to an individual will be assessed against the risk criteria outlined in the department's Privacy and Data Breach Procedures, which can be found in the department's privacy management plan.

What data or information does this policy cover?

This policy covers any record of personal and health information which is:

- held by the department, or
- is contained in a record for which the department is responsible under the *State Records Act 1998.*

How do I report?

Report a breach by using the portal on the Privacy and Confidentiality page on Compass, or contacting the Information Access & Privacy team (Privacy team) via privacy@dpie.nsw.gov.au or 02 9860 1440.

What happens after reporting?

The Privacy team, in consultation with the relevant business unit(s), will assess the breach and provide advice as to what, if any, action needs to be taken. The Privacy team will assist the relevant business unit to undertake remedial action to meet the department's statutory obligations. Detailed information is available in the department's Privacy and Data Breach Procedure. The procedure is set out in the department's privacy management plan.

If the breach meets the threshold of an 'eligible data breach', the department will notify the NSW Privacy Commissioner and either:

- notify each affected individual(s), or
- publish a notification and take reasonable steps to publicise the incident.

Am I personally responsible?

The legislation does not hold individual employees liable for a breach that occurs in the course of their ordinary working duties and **when acting in good faith** . It is important to be careful when handling any personal information.

It is, however, an offence to, or to offer to, intentionally access, use or disclose information, or try to get another officer to use or disclose information, that is outside of the normal exercise of your duties.

If you inappropriately access or disclose information when it is not necessary for the exercise of your duties, this may be considered a breach of the Code of Ethics and Conduct, and could result in disciplinary action being taken against you.

Early intervention helps the department manage the aftermath of any breach and is critical to mitigating or preventing any damage that may occur. Swift, proactive reporting is essential.

Failure to comply with this policy

All employees are expected to comply with the department's Code of Ethics and Conduct which requires you to act in accordance with this policy. Failure to comply may result in corrective action including misconduct action.

Roles and responsibilities

Roles	Responsibilities
All employees, volunteers, contractors and contingent labour	• Handle personal information in accordance with the PPIP Act. • Take steps to ensure external stakeholders comply with our privacy requirements. • Report all breaches and suspected breaches. • Assist the privacy team in investigating and assessing breaches, and with any internal reviews that result.

Roles	Responsibilities
Managers	• Ensure staff are aware of their obligation under this Policy • Encourage employees to the report all breaches and suspected breaches.
Information Access & Privacy unit (Privacy team)	• Liaise with the Privacy Commissioner • Maintain the notifiable breach register. • Provide services, support, advice and information to staff and managers to assist them to comply with their obligations.

Key definitions

Terms	Definitions
Affected individual	An individual to whom the information, that is subject to a data breach, relates.
Privacy breach	Action or inaction that results in a failure to comply with the Information Protection Principles set out in the PPIP Act or the Health Privacy Principles set out in the HRIP Act.
Eligible data breach	Term used in the PPIP Act to describe a privacy breach that requires notification under the mandatory notification of data breach scheme.

Terms	Definitions
Health information	Health information is defined in section 6 of the *Health Records and Information Protection Act 2002*: *In this Act,* ***health information*** *means—* *(a) personal information that is information or an opinion about—* *(i) the physical or mental health or a disability (at any time) of an individual, or* *(ii) an individual's express wishes about the future provision of health services to him or her, or* *(iii) a health service provided, or to be provided, to an individual, or* *(b) other personal information collected to provide, or in providing, a health service, or* *(c) other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances, or* *(d) other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of a genetic relative of the individual, or* *(e) healthcare identifiers,* *but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of this Act generally or for the purposes of specified provisions of this Act.*
Personal information	Personal information is defined in section 4 of the PPIP Act: *In this Act,* ***personal information*** *means information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.* Section 4(3) lists things that are not personal information, such as information about an individual that is contained in a publicly available publication.
Record	A record means any document or other source of information compiled, recorded or stored in written form or on film, or by electronic process, or in any other manner or by any other means (section 3, *State Records Act 1998*).
Serious harm	Each data breach will be assessed against the risk criteria in the Privacy and Data Breach Procedures to determine the likely harm to affected individuals.

Related documents

The PPIP Act is the legislation that should be read in conjunction with this policy. Other policy documents that should be read in conjunction with this policy are:

- Privacy Management Plan (PMP)
- The departmental Privacy Statement
- Privacy statements on branded websites within the departmental network, such as the NSW Planning Portal, the National Parks and Wildlife website, or the Sydney Olympic Park Authority
- Breach Notification Procedure
- Instrument of Delegation
- Cyber security policy
- Information Technology Response Plan
- Code of Ethics and Conduct.pdf
- Records and Information Management policy.pdf
- Acceptable Use Policy.pdf

Policy metadata

Category	Description
Status	Draft
Date of approval	28 November 2023
Approver	General Counsel - Deputy Secretary
Group	Governance and Legal
Division	Governance
Policy owner	Director Corporate Governance
Branch	Corporate Governance
Document location	DPE Intranet and external DPE policy website
Next review date	November 2024 (desktop review)
Associated procedure	Confidentiality and privacy (sharepoint.com)

Category	Description
Any additional applicability	This policy applies to the Department of Planning & Environment and all portfolio sub-agencies listed in Appendix 1 of the department's Privacy Management Plan. This policy does not apply to those not listed in Appendix 1 of the department's Privacy Management Plan.
Superseded document	None
Further information	Contact Information Access & Privacy on 02 9860 1440 or privacy@dpie.nsw.gov.au

Version control

Version	Date issued	Change
1.0	27 November 2023	