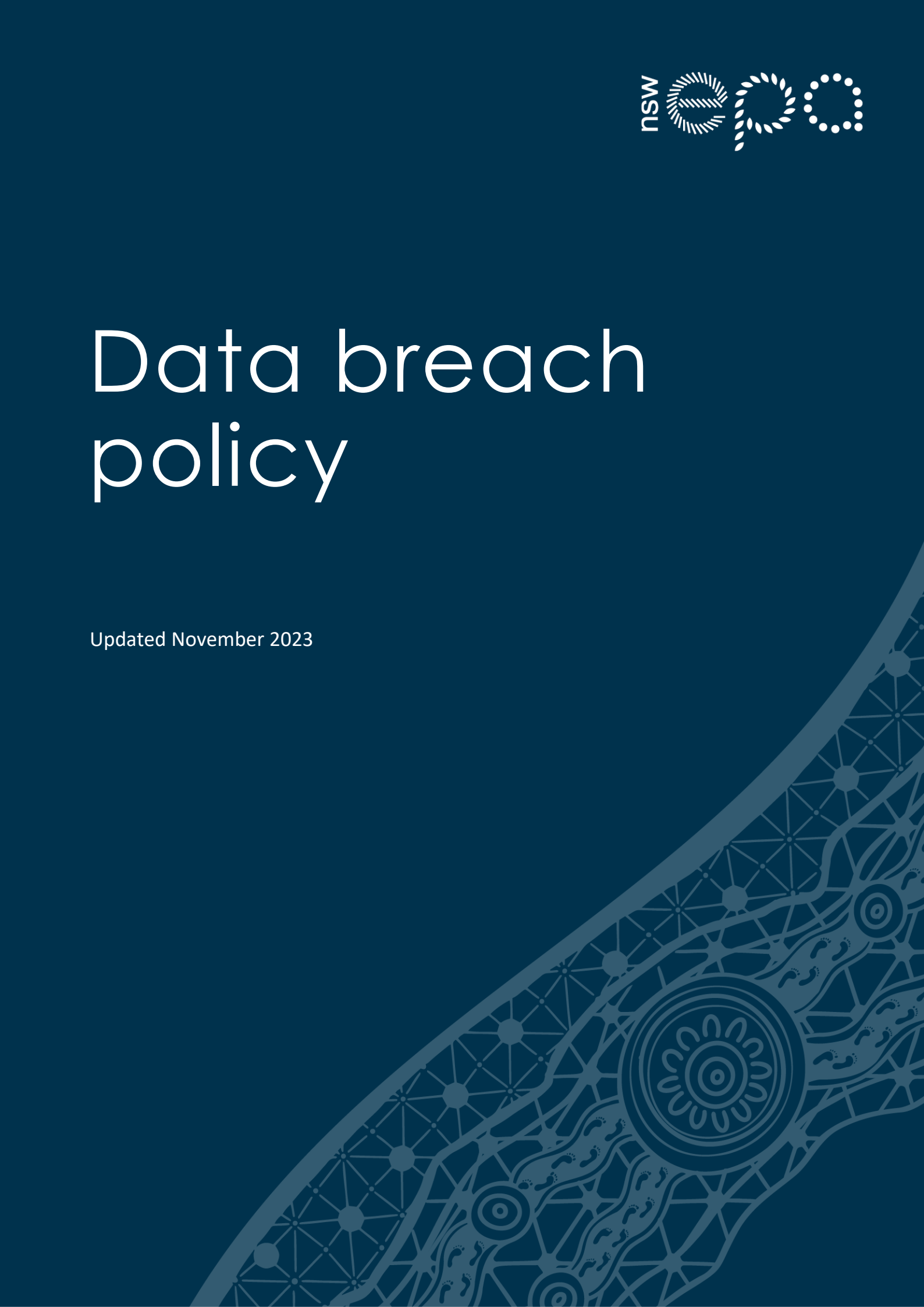
Data breach policy

Updated November 2023



Acknowledgement of Country

The NSW Environment Protection Authority acknowledges the Traditional Custodians of the land on which we live and work, honours the ancestors and the Elders both past and present and extends that respect to all Aboriginal people.

We recognise Aboriginal peoples' spiritual and cultural connection and inherent right to protect the land, waters, skies and natural resources of NSW. This connection goes deep and has since the Dreaming.

We also acknowledge our Aboriginal and Torres Strait Islander employees who are an integral part of our diverse workforce and recognise the knowledge embedded forever in Aboriginal and Torres Strait Islander custodianship of Country and culture.

Published by:
NSW Environment Protection Authority

6&8 Parramatta Square
10 Darcy Street,
Parramatta NSW 2150
Locked Bag 5022,
Parramatta NSW 2124

Phone: +61 2 9995 5000 (switchboard)
Phone: 131 555
(NSW only – environment information and publications requests)

Fax: +61 2 9995 5999

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

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

Email: info@epa.nsw.gov.au
Website: www.epa.nsw.gov.au

Report pollution and environmental incidents
Environment Line: 131 555 (NSW only) or info@epa.nsw.gov.au
See also www.epa.nsw.gov.au

ISBN 978 1 922963 69 7
EPA 2024P4520
May 2024

1. Introduction

Part 6A of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) establishes the NSW Mandatory Notification of Data Breach Scheme. The scheme requires every NSW public sector agency bound by the PPIP Act, including the Environment Protection Authority (EPA), to notify the Privacy Commissioner and affected individuals of an 'eligible data breach'.

Under the scheme, public sector agencies are required to prepare and publish a data breach policy for managing such breaches.

2. Data breach policy

2.1. Purpose

This data breach policy outlines the EPA's approach to complying with the Mandatory Notification of Data Breach Scheme including roles and responsibilities for:

- containing, assessing and managing data breaches, and
- notifying and reporting on 'eligible data breaches'.

Effective breach management, including notifications, assists the EPA in avoiding or reducing possible harm to both the affected individuals/organisations and the EPA, and may prevent future breaches.

2.2. Scope

This policy applies to:

(a) any records involving personal or health information held by the EPA, or

(b) information contained in a State record in respect of which the EPA is responsible under the *State Records Act 1998*.

The Policy applies to:

- all EPA employees, including ongoing, term, temporary, casual employees or seconded employees, contingent workers, volunteers and consultants, and
- any third-party providers, contractors or agencies who hold personal and health information on behalf of or jointly with the EPA.

This policy does not apply to data breaches that:

- do not involve personal or health information, or
- Are not likely to result in serious harm to an individual.

2.3. Failure to comply with this policy

Breaches of this policy by employees will be managed according to the Fraud and Corruption Control Policy (2022) and section 69 of the *Government Sector Employment Act 2013*.

Guidance can be found in the EPA Code of Ethics and Conduct (2022) and the Managing Misconduct policy 2022.

2.4. Key terms

2.4.1. What is a data breach?

A data breach happens when personal information held by an agency (whether in digital or hard copy) 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.

Data breaches may be caused by:

- **Human error**
    - When a letter or email is sent to the wrong recipient
    - When system access is incorrectly granted to someone without appropriate authorisation
    - When a physical asset such as a paper record, laptop, USB stick or mobile phone is lost or misplaced
    - When staff fail to implement appropriate password security, for example not securing passwords or sharing password and log in information
    - When personal or health data is disclosed to or shared with unauthorised recipients.
- **System failure**
    - Where a coding error allows access to a system without authentication, or results in automatically generated notice that includes incorrect information or is sent to incorrect recipients
    - Where systems are not maintained through the application of known and supported patches.
- **Malicious or criminal attack**
    - Cyber incidents such as ransomware, malware, hacking, phishing or brute force access attempts resulting in access to or theft of personal information
    - Social engineering or impersonation leading to inappropriate disclosure of personal information
    - Insider threats from agency employees using their valid credentials to access or disclose personal information outside the scope of their duties or permissions.

2.4.2. What is an eligible data breach?

The Mandatory Notification of Data Breach Scheme applies where an 'eligible data breach' has happened. For a data breach to constitute an 'eligible data breach' under the scheme, there are two tests to be satisfied**:**

1. There is an unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency or there is a loss of personal information held by a public sector agency in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information, **and**
2. A reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates.

An eligible data breach may involve:

- unauthorised access to data by an EPA employee or by an external person or entity, and/or
- unauthorised disclosure of information externally, publicly or internally.

Section 59H of the PPIP Act provides a non-exhaustive list of factors an assessor may consider when assessing whether a data breach is an eligible data breach for the purpose of the Mandatory Notification of Data Breach Scheme. These include:

- the types of personal information involved, and whether a combination of types of personal information might lead to increased risk
- the level of sensitivity of the personal information assessed, disclosed or lost
- whether the personal information is or was protected by security measures such as encryption and therefore unlikely to be accessed or misused
- the amount of time the information was exposed or accessible, including the amount of time information was exposed before the agency discovered the breach
- the circumstances in which the breach happened
- actions taken by the agency to reduce the risk of harm following the breach, and
- any other matter specified in the Privacy Commissioner's guidelines.

2.4.3. What is 'personal information'?

Under section 4 of the PPIP 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(2) of the PPIP Act provides that personal information includes things such as an individual's fingerprints, retina prints, body samples or genetic characteristics.

Section 4(3) of the PPIP Act provides a list of information that is not personal information, such as information about an individual that is contained in a publicly available publication.

2.4.4. What is 'health information'?

Section 59B of the PPIP Act provides that ***personal information*** includes health information within the meaning of the *Health Records and Information Protection Act 2002.*

Under section 6 of the *Health Records and Information Protection Act 2002*, ***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.

2.4.5. What is 'serious harm'?

The term ***'serious harm'***, although not defined in the PPIP Act, means harm arising from the eligible data breach that has, or may have, a real and substantial detrimental effect on an individual. The effect on the individual must be more than mere irritation, annoyance or inconvenience.

Harm to an individual includes physical harm, economic, financial, or material harm, emotional or psychological harm or reputational harm. It also includes other forms of serious harm that a reasonable person in the EPA's position would identify as a possible outcome of the data breach.

The assessor will consider the circumstances of the breach, how likely it is that the breach will cause harm and the consequences and severity of that harm.

2.5. Roles and responsibilities

Roles	Responsibilities
All EPA employees, contingent workers, volunteers and consultants	• Handle personal information in accordance with the *Privacy and Personal Information Protection Act* • Handle health information in accordance with the *Health Records and Information Privacy Act 2002* • Ensure the safe custody and proper preservation of State records in accordance with the *State Records Act 1998* • Carry out required training on handling personal and health information • Take steps to ensure external stakeholders comply with the EPA's privacy requirements • Report all data breaches and suspected data breaches • Assist with investigating and assessing breaches, and any resulting internal reviews.
EPA Risk & Governance team	• Liaise with the NSW Information and Privacy Commission and affected individuals • Maintain an internal register for eligible data breaches • Maintain a public register of data breach notifications issued • Review and update this policy • Review and update policy and procedure documents including the EPA's Privacy Management Plan.
Executive Director Legal, Governance and People and Director - Governance, Risk & Planning	• Carry out or direct one or more persons to carry out an assessment of a data breach • Decide the nature of a data breach and the risks associated with the breach to determine next steps • Provide instruction to mitigate the harm done by the suspected breach • Approve extension of the period to conduct the assessment • Report eligible data breaches to the EPA Chief Executive Officer (CEO) • Any other functions that are authorised by the EPA CEO in accordance with the CEO delegation instrument.
Directors, Managers	• Make all reasonable efforts to contain a data breach and attempt recovery of any lost information • Ensure staff comply with training requirements on handling personal and health information • Help with incident review and preventative efforts, based on the type and seriousness of the breach.

3. Responding to data breaches

3.1. Prepare for a data breach

3.1.1. Training

- All EPA employees must complete their annual code of ethics and conduct training and cyber security training which incorporates information on the Mandatory Notification of Data Breach Scheme
- All EPA employees, contingent workers, volunteers and consultants must be familiar with the EPA's Privacy Management Plan
- EPA employees, contingent workers, volunteers and consultants are strongly encouraged to visit the NSW Information and Privacy Commission website and review resources available on the Mandatory Notification of Data Breach Scheme, including attending the online webinar introducing the scheme
- The EPA will continue to review the training needs of staff with respect to data breaches and provide training on reporting, managing and responding to data breaches.

3.1.2. IT network management and cyber security system

The EPA's IT network management and cyber security system is provided and managed by Department of Planning, Housing and Infrastructure's Digital Information Office (DIO). The EPA's Digital Data and Intelligence branch is responsible for liaison with the DIO.

3.1.3. Outsourcing and collaborations

The EPA will take steps to make sure all third-party providers (including external service providers or other agencies) who store personal or health information on behalf of or jointly with the EPA are aware of the Mandatory Notification of Data Breach Scheme and the obligations under this policy to report any eligible data breaches to the NSW Privacy Commissioner.

3.2. Responding to a data breach

The EPA will employ five key steps in responding to a data breach:

1. Initial report and triage
2. Contain the breach
3. Assess and mitigate the breach
4. Notify
5. Review

The first four steps will be carried out at the same time where possible. Details of each step are set out in the EPA's Data Breach Response Plan.

As soon as a breach is identified, EPA staff are required to report to their Executive Officers or above within one business day regardless of how serious or minor it might be.

The EPA takes a precautionary approach, and all breaches are consistently and thoroughly assessed to make sure we fulfill our reporting and notification obligations. Early reporting helps the EPA contain a breach and mitigate any potential harm.

The EPA will immediately make all reasonable efforts to contain a data breach to prevent any further compromise of personal or health information.

An assessor will be appointed to carry out the assessment of whether the data breach is eligible, or there are reasonable grounds to believe it is. The assessor must take reasonable steps to complete the assessment within 30 calendar days. This timeframe might be extended if the Executive Director Legal Governance and People or Director Governance Risk and Planning is satisfied that completing the assessment within 30 days is not possible. The NSW Privacy Commissioner will be notified if this is the case.

If the data breach is assessed and meets the criteria of an eligible data breach, the EPA will notify:

- the NSW Privacy Commissioner and,
- each individual to whom the personal information the subject of the breach relates, or each affected individual (exemptions are available under Division 4 of Part 6A of the PPIP Act).

If the EPA is unable to notify any or all of the individuals specified above, or if it is not reasonably practicable to, the EPA will issue a public notification of the eligible data breach. A record of any public notification of an eligible data breach will be published on the EPA's website and recorded on the public notification register for a period of twelve months.

The EPA will further investigate the circumstances of any breach to determine all relevant causes and consider whether changes to systems, processes and procedures are needed to mitigate future risks. This will make sure the EPA continues to proactively manage data breaches in line with regulator and community expectations.

3.3. Other obligations including external engagement or reporting

The EPA may also be required by contract or by other laws or administrative arrangements to notify other third parties to take specific steps in response to a data breach. These may include taking specific containment or remediation steps, or engaging with or notifying external stakeholders, where a data breach happens.

Notification to other parties could include:

- NSW Police Force and/or Australian Federal Police, where the EPA suspects a data breach is a result of criminal activity
- Cyber Security NSW, the Office of the Government Chief Information Security Officer and The Australian Cyber Security Centre, where a data breach is a result of a cyber security incident
- The Office of the Australian Information Commissioner, where a data breach may involve agencies under the Federal jurisdiction
- Any third-party organisations or agencies whose data may be affected
- Financial services providers, where a data breach includes an individual's financial information
- Professional associations, regulatory bodies or insurers, where a data breach may have an impact on these organisations, their functions and their clients
- The Australian Cyber Security Centre where a data breach involves malicious activity from a person or organisation based outside Australia.

3.4. Breaches involving more than one agency

The EPA might hold information jointly with other agencies, and there may be situations in which the breach of personal or health information held by one agency must be managed across multiple agencies.

For example, where one agency has physical custody of the record, while a second agency retains authority to determine what is done with the records.

In the event of a data breach affecting personal information that is jointly held between agencies, each agency is required to assess the breach and if the breach is determined to be an eligible data breach, each agency must notify the NSW Privacy Commissioner. However, only one of the affected agencies is required to notify affected individuals or make a public notification (if required).

The EPA will directly liaise with other affected agencies in respect of any notification requirements for the data breach. In general, the agency with the most direct relationship with the affected individuals will be best placed to notify and provide direct support as required.

3.5. Breaches involving private sector service providers

Information is 'held' by an agency if the agency is in 'possession' or 'control' of the information. This means that information in the hands of a private sector service provider may still be 'held' by the EPA if the EPA retains a legal or practical power to deal with the personal information – whether or not the EPA physically possesses or owns the medium on which the personal information is stored.

The EPA's Director Digital Data and Intelligence will assist the Executive Director Legal Governance and People or Director Governance Risk and Planning to coordinate with private sector service providers to address and respond to identified data breaches related to any EPA IT systems.

4. Are EPA employees personally responsible?

The legislation does not hold individual employees liable for a breach that happens in the course of their ordinary working duties and when acting in good faith. The EPA encourages employees to be transparent and emphasises the obligation to report a breach or any suspected breaches immediately. Early intervention helps control the situation and is essential for mitigating or preventing any damage that may happen.

It is, however, an offence to, or to offer to, intentionally access, use or disclose information, or ask 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 EPA's Code of Conduct and Ethics and misconduct action may be taken against you.

5. Other legislation

Under Schedule 1 of the *Government Information (Public Access) Act 2009*, it is to be conclusively presumed that there is an overriding public interest against disclosure of information contained in a document

prepared for the assessment of an eligible data breach under Part 6A of the PPIP Act, if the information could worsen a public sector agency's cyber security or lead to further data breaches.

6. Review of this policy

This policy will be reviewed annually or where improvements are identified in response to a data breach; whichever happens sooner.

7. Related documents

The PPIP Act should be read with this policy. Other policy documents that should be read in with this policy include:

- EPA Privacy Management Plan
- EPA Instrument of Delegation for the Mandatory Notification of Data Breach Scheme
- EPA Data Breach Response Plan
- EPA Code of Conduct and Ethics
- EPA Statement of Business Ethics
- DPE Records Management Policy
- DPE Information and Communication Technology Acceptable use Policy.