Data Breach Policy and Guide

1 Policy statement

IPART understands that data breaches involving personal or health information can have serious consequences for individuals. We are committed to responding to a data breach in a manner that mitigates the potential harm to individuals from a breach, is quick, effective and transparent.

Part 6A of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) establishes the NSW Mandatory Notification of Data Breach (MNDB) scheme. The MNDB scheme requires every NSW public sector agency bound by the PPIP Act to notify the Privacy Commissioner and affected individuals of eligible data breaches.

This policy outlines IPART's approach to complying with the MNDB scheme, the roles and responsibilities for reporting data breaches and the way IPART responds to data breaches, including assessing, managing and notifying eligible data breaches in order to reduce the risk of harm to affected individuals and our staff.

2 Scope and purpose

This policy applies to:

- all staff, Tribunal and Committee members and contractors of IPART. This includes temporary and casual staff, private contractors and consultants engaged by IPART to perform the role of a public official.
- third party providers who hold personal and health information on behalf of IPART.

The policy details:

- what constitutes an eligible data breach under the PPIP Act
- roles and responsibilities for reporting, reviewing and managing data breaches
- the steps that IPART will take to respond to a data breach and review systems, policies and procedures to prevent future data breaches.

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

3 Roles and responsibilities

Table 1 provides a summary of the roles and responsibilities at IPART in the event of a data breach.

Table 1 Roles and responsibilities

Role	Key responsibilities
All staff	• Immediately report a potential data breach and provide information about the data breach to their manager and the Privacy Officer or Principal Risk Officer. • Protect all personal information held against unauthorised disclosure or use.
Managers	• Provide support to the employee/s that may have caused the data/ privacy incident. • Support and participate in the Data Breach Response Team to provide information and actions in response to the data/ privacy incident. • Provide input to the Privacy Officer and/or Data Breach Response Team for any briefing notes, letters or correspondence that needs to be drafted in response to the data/ privacy incident, • Manage records of all responses from individuals who were affected by the incident
Privacy Officer	• Report a suspected eligible data breach to the Chief Executive Officer (as delegate of the Chair) • Ensure Data Breach Policy and processes and procedures including registers and form templates are incorporated in IPART's policies and practices. • Review and recommend updates to the Data Breach Policy as required. • Ensure compliance with all IPART policies and procedures including the Privacy Management Plan and Data Breach Policy • Support the Privacy Management Plan through awareness-building, skills development, and user training. • Assemble the Data Breach Response Team • Coordinate recordkeeping for each data breach, including maintenance of the IPART Data Breach Registers
Chair (CEO as their delegate)	• Ensure Data Breach Policy is implemented across IPART. • Ensure data breach response and risk management strategies are appropriate and effective. • Make the Privacy Management Plan and Data Breach Policy publicly available. • Confirm support for data breach responsibilities in the Code of Ethics and Conduct. • Approve the release of the Data Breach Policy as required. • Receive notification of suspected eligible data breaches. • Direct the Privacy Officer, Data Breach Response Team or another person to assess suspected eligible data breaches. • During assessment of the breach, make all reasonable attempts to mitigate the harm done by the suspected breach (including by instructing the Data Breach Response Team and other staff). • Notify the Privacy Commissioner of the eligible data breach and affected individuals **Note**: The Chair has delegated their functions as the head of agency under the MNDB scheme to the CEO.[a]
Legal Team	On request, advise relevant stakeholders within IPART whether an eligible data breach has occurred and on IPART's obligations to respond to eligible data breaches.
Data Breach Response Team	• A team will be assembled to respond to and manage any suspected eligible data breach • Assess and develop and implement actions to mitigate suspected eligible data breaches • Identify the information that was accessed or disclosed and all affected individuals • Identify the cause of the data breach • Identify process and control issues to ensure data breach is contained and take all appropriate actions to remediate it • Coordinate IPART's response to a suspected eligible data breach to the CEO

[a] D23/25669.

4 Our commitment

IPART has established systems and processes for preventing and managing data breaches.

IPART provides training and resources to staff and other people subject to this Policy and the Data Breach Response Procedure to help them prevent, identify and report potential data breaches.

IPART's network and infrastructure is managed by GovConnect (DCS) who have implemented cyber security measures to mitigate the risk of data breaches. This includes cyber security projects to increase cyber security maturity, regular cyber security and privacy training for all staff (including threat trends) and procedures for sharing of personal and sensitive information.

IPART will ensure that, in contracts that involve suppliers handling personal or health information on behalf of IPART, there are appropriate contractual provisions in place that require the supplier to handle personal information appropriately and securely and to assist IPART in dealing swiftly and effectively with a data breach.

IPART maintains an internal register of eligible data breaches and also maintains and publishes a public register of any notifications made under section 59N(2) on our website.

IPART includes cyber security incidents (which may involve a data breach) in our Risk Register and established controls to mitigate the risk and impact on our systems, data holdings and individuals. The loss of IT systems as a result of a cyber security incident is included in IPART's Business Continuity Plan.

IPART will continue to proactively manage data breaches in line with regulator and community expectations. To assist in preventing and mitigating future breaches, IPART will conduct post-breach reviews and evaluations to understand the cause of a data breach and, where appropriate, implement recommended changes to systems and policies.

5 Data Breaches

5.1 What is an eligible data breach?

An 'eligible data breach' occurs where:

- either:
  - there is unauthorised access to, or unauthorised disclosure of, personal information or health information held by IPART, or
  - personal information held by IPART is lost in circumstances where the loss is likely to result in unauthorised access or unauthorised disclosure, and
- a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to an individual to whom the information relates.

An eligible data breach must be reported to the NSW Privacy Commissioner under the MNDB scheme. Affected individuals must also be notified. The MNDB scheme applies to eligible data breaches of:

- '**personal information**', meaning information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.
- '**health information**', which includes personal information that is information or an opinion about an individual's physical or mental health, disability, and information connected to the provision of a health service.

Section 9 of this Policy sets out the definitions of personal information and health information in full.

Data breaches can occur because of a technical problem, human error, inadequate policies and training, a misunderstanding of the law or a deliberate act. Data breaches may happen when personal information is lost, stolen, or mistakenly disclosed.

Examples of data breaches include:

- 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 containing personal information is lost, misplaced or stolen
- social engineering or impersonation leading into inappropriate disclosure of personal information
- cyber incidents such as ransomware, malware, hacking, phishing or brute force access attempts resulting in access to or theft of personal information.

5.2 Potential impact of data breaches

The impact of data breaches depends on the nature and extent of the breach and type of data that has been compromised.

A data breach can result in serious harm to an impacted individual whether the breach affects one person or several thousand.

Harm can be physical, psychological, emotional, financial or reputational e.g, identity theft, financial loss, blackmail, threats to personal safety, humiliation, stigma, embarrassment, damages to reputation or relationships.

IPART may also be negatively impacted by a data breach and may experience reputational damage, financial loss, loss of public trust or services it provides.

5.3 Reporting of data breaches

All data breaches or suspected data breaches identified by IPART staff must be reported immediately to their manager and Privacy Officer or Principal Risk Officer.

Information about how to report and what information should be provided as part of a report is available in the Data Breach Response Procedure.[b]

Staff must report all data breaches, including any breaches that have already been contained e.g. if a stolen laptop has been recovered, or lost hard copy files returned.

Members of the public can also report actual or suspected data breaches to IPART. To do so, members of the public should email ipart@ipart.nsw.gov.au

6 Data breach response procedure

IPART staff must respond to a data breach in accordance with the Data Breach Response Procedure.[c] If the data breach is also an ICT incident or cyber security incident, staff must also respond in accordance with ICT Incident Management Plan.[d]

The response to a data breach will involve:

1. **Report and contain–** all data breaches identified by staff or communicated to staff by a member of the public must be reported immediately to their manager and Privacy Officer or Principal Risk Officer (see section 5.3 for further details on reporting of data breaches). The CEO and any staff instructed by the CEO will immediately make all reasonable efforts to contain the breach and carry out preliminary fact-finding.
2. **Assess and mitigate** – the CEO will direct the Privacy Officer, Data Breach Response Team or another staff member to assess the breach and the likelihood that the breach will result in serious harm to an individual to whom the information relates (that is, to determine whether the breach is an 'eligible data breach'). Simultaneously, steps will be taken with the aim of mitigating harm resulting from the breach.
3. **Notify –** if the assessment concludes that the breach is likely to result in serious harm to an individual to whom the information relates (and so is an eligible data breach), the CEO will immediately notify:
   a. the NSW Privacy Commissioner of the breach and,
   b. unless an exemption applies (see section 7), individuals to whom the information relates (including affected individuals).

   If the CEO is unable to notify, or where it's not reasonably practicable to notify, any or all individuals whose personal information was subject of the breach or affected individuals, the CEO will publish a notification on the IPART website in its public notification register, and will take reasonable steps to publicise that notification. The CEO may also choose to publish notice of eligible data breaches on the register where all affected individuals have been notified.

   As soon as practicable after a notification is published on IPART's public notification register, the Privacy Officer must provide the Privacy Commissioner with information about how to access the notification on the public notification register.

[b] D23/30861.

[c] D23/30861.

[d] D22/26938.

If the data breach involves tax file numbers, IPART will notify the Australian Information Commissioner if required by the *Privacy Act 1988* (Cth). If the breach is not an eligible data breach, the CEO may consider notifying individuals and the NSW Privacy Commissioner.

4. **Review -** a review of the breach will be carried out, including to identify steps that may be taken to prevent future breaches. All eligible data breaches will be added to IPART's internal data breach register, as required under the PPIP Act.

The Data Breach Response Team will coordinate IPART's response to the breach. If the data breach is also an ICT incident or cyber security incident, the same response team may be formed to deal with the incident under both the ICT Incident Management Plan[e] and the Data Breach Response Procedure.

7 Where we may not notify

We may not notify individuals to whom information affected by a data breach relates or the public where:

- multiple agencies are involved in an eligible breach and another agency has notified affected individuals
- the CEO reasonably believes notification of the eligible data breach would be likely to prejudice an ongoing investigation or court/tribunal proceedings
- IPART has taken action to mitigate the data breach before it results in serious harm or loss to an individual and that action prevents the harm or loss
- notification would be inconsistent with secrecy provisions of other legislation
- notification would create a serious risk of harm to an individual's health or safety
- the CEO reasonably believes that notification would worsen IPART's cyber security or lead to further data breaches.

8 Record-keeping requirements

The Privacy Officer coordinates record-keeping for each data breach, including maintenance of the IPART Internal Data Breach Register and public notification register (published on website).

All responsible officers involved in a data breach will maintain appropriate records to provide evidence of how suspected breaches are managed, including those not escalated to the response team or notified to the Privacy Commissioner.

[e] D22/26938.

9 Definitions

Table 2 provides a glossary of key terms used in this document.

Table 2 Definitions

Term	Definition
Affected individual	As defined in section 59D(2) of the PPIP Act, an individual specified in section 59D(1)(a) or (1)(b)(ii) of the PPIP Act. That is, an individual to whom information involved in a data breach relates who a reasonable person would conclude is likely to experience serious harm.
Data breach	• Where there is unauthorised access to, or unauthorised disclosure of, personal or health information held by IPART. • Where personal or health information held by IPART is lost in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur.
Eligible data breach	As defined in section 59D(1) of the PIPP Act, eligible data breach means - (a) there is unauthorised access to, or unauthorised disclosure of, personal information held by IPART and 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, or (b) personal information held by IPART is lost in circumstances where— (i) unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and (ii) if the unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to an individual to whom the information relates.
Health information	As defined in section 6 of the HRIP Act, health information is: • personal information that is information or an opinion about: – the physical or mental health or a disability (at any time) of an individual (such as a psychological report, blood test or x-ray) – an individual's express wishes about the future provision of health services to him or her, or – a health service provided, or to be provided, to an individual, or • other personal information collected to provide, or in providing, a health service, or • 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 • 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 • healthcare identifiers.
Personal information	• As defined in 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. Personal information can include: – person's name, address, financial information and other details – photographs, images, video or audio footage, and – individual's fingerprints, retina prints, body samples or genetic characteristics. • For the purposes of Part 6A of the PPIP Act (Mandatory notification of data breaches), personal information includes health information within the meaning of the HRIP Act.
Suspected eligible data breach	Where there are reasonable grounds to suspect there may have been an eligible data breach.

10 Related documents

This policy should be read with:

- IPART Data Breach Response Procedure[f]
- Internal Data Breach Register[g]
- Public Notification Register[h]
- IPART Privacy Management Plan[i]
- Privacy and Personal Information Protection Act 1988 (NSW)
- Information and Privacy Commission NSW – Data breach guidance
- Incident Management Plan[j]
- ICT Incident Management Plan[k]

11 Monitoring and review

This Policy is a managed document. Changes will be issued as a complete replacement document. This Policy will be reviewed, at a minimum every 2 years, or in response to material changes in the operating environment.

Implementation date: November 2023

Contact: Privacy Officer
Email: ipart@ipart.nsw.gov.au
Post: IPART, PO Box K35, Haymarket Post Shop, NSW 1240
Phone: 02 9290 8400

Title	Data Breach Policy and Guide
Approver	Chief Executive Officer
Version	Version 1
Effective Date	28 November 2023
Owners	Privacy Officer (Executive Office Manager)
Reference	23/1284
Approval	21 November 2023
Review Date	28 November 2025

[f] D23/30861
[g] D23/31154
[h] D23/31153
[i] W21/3936
[j] D22/26937
[k] D22/26938