# Data Breach Policy

Printed copies of this document may not be up to date. Ensure you have the latest version before using this document.

# Table of Contents

# Contents



# Policy overview

## Scope and purpose of this policy

This Data Breach Policy provides guidance to Staff when responding to data breaches, in accordance with the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act) and *Health Records and Information Privacy Act 2002* (NSW) (HRIP Act).

The PPIP Act and HRIP Act have strict controls around how public sector agencies handle personal information and health information. Data breaches occur when there is any unauthorised access, use, disclosure, or loss of that personal or health information.

Part 6A of the PPIP Act establishes the mandatory notification of data breach (MNDB) scheme, which requires that Legal Aid NSW report to the Privacy Commissioner any Eligible Data Breach that may occur within the organisation.

The MNDB scheme also requires that Legal Aid NSW prepare, publish, and make publicly available a Data Breach Policy.

The scope and purpose of this Data Breach Policy is therefore to ensure Staff comply with both:

1. the MNDB scheme in dealing with Eligible Data Breaches; and
2. Legal Aid NSW procedures in responding to all data breaches.

## Applicability and target groups

All Staff must comply with this Policy.

Managers should ensure that all relevant staff members know about this policy and how to apply it. If anything in this policy is unclear, or you are unsure about how to apply the policy, contact the person listed on the cover page of this policy.

### Legislative environment

This policy takes into account the obligations set under the PPIP Act and HRIP Act, and the confidentiality provisions under sections 25 and 26 of the *Legal Aid Commission Act 1979* (NSW).

## Definitions and abbreviations

**Affected Person** – an individual whose personal or health information is subject to a data breach. This may also include an affected organisation in relation to a Serious Breach.

**DFV Connect** – WDVCAS Client and Case Management System (DFV Connect) that is used to manage the records of clients who have been provided services by WDVCAS providers.

**Eligible Data Breach** – see part 1.

**Formal Complaint** – A data breach that is not a Serious Breach or Eligible Data Breach but involves a formal/written complaint, an internal or external privacy review, or a court or tribunal action.

**Health Information** – see s 6 of the HRIP Act.

**HRIP Act** – *Health Records and Information Privacy Act 2002* (NSW).

**IPC** – Information and Privacy Commission NSW

**Minor Incident** – A data breach that is not a Formal Complaint or Serious Breach or Eligible Data Breach. It is accidental or the result of a systems error; and involves a small number of documents and individuals.

**MNDB scheme** – Mandatory Notification of Data Breach scheme under Part 6A of the PPIP Act.

**Other Data Breach** – any Minor Incident, Formal Complaint, or Serious Breach that is not an Eligible Data Breach.

**Personal Information** – see s 4 of the PPIP Act.

**PPIP Act** – *Privacy and Personal Information Protection Act 1998* (NSW).

**Privacy Legislation** – PPIP Act and HRIP Act.

**Privacy Officer** – Manager, In-house Counsel Unit.

**Serious Breach** – see part 5.

**Staff** – all Legal Aid NSW staff, and in relation to DFV Connect records, all WDVCAS and Family Advocacy and Support Service (FASS) staff.

**WDVCAS** – Women's Domestic Violence Court Advocacy Service.

## Monitoring, evaluation and review

This document is to be reviewed every 2 years, or as otherwise required following a post data breach review. This Policy commenced in November 2023.

## Further information, additional resources & associated documents

This policy should be read in conjunction with the Legal Aid NSW Privacy Management Plan and Legal Aid NSW Privacy Policy, and for staff the Cyber Security Intranet Page.

Depending on the circumstances, non-compliance with this Policy may constitute a breach of employment or contractual obligations or misconduct under the Legal Aid NSW Code of Conduct.

## 1. What is a data breach?

A data breach occurs when any personal information or health information held by Legal Aid NSW is:

- Accessed, used, or disclosed without authorisation;
- Sent to the wrong recipient; or
- Lost.

A data breach can be accidental, inadvertent, intentional, or malicious. It can also be minor or serious.

An accidental or inadvertent data breach may be the result of human error, for example where a staff member leaves their laptop on a train, or an email or letter containing a client's personal information is sent to the wrong address. A data breach may also arise from a technical or administrative systems failure.

Legal Aid NSW has two main categories we use to classify data breaches:

1. Eligible Data Breaches; and
2. Other Data Breaches.

(Together referred to as a "data breach")

**Eligible Data Breaches** refer to data breaches where there is (or if the information is lost, likely to be) unauthorised access to, or disclosure of, personal or health information held by Legal Aid NSW, and a reasonable person would conclude that this is likely to result in serious harm to an individual to whom the information relates. These breaches fall under the MNDB scheme.

**Other Data Breaches** include a Minor Incident, Formal Complaint, or a Serious Breach that is not an Eligible Data Breach. These breaches fall outside the MNDB scheme.

If we suspect that a breach may be an Eligible Data Breach, but it has not yet been assessed under the MNDB scheme, we will still consider it to be an Eligible Data Breach. However, if after assessment we decide that it is not an Eligible Data Breach, it will then be considered an Other Data Breach.

## 2. The 7 steps Legal Aid NSW takes when responding to a data breach

Staff commence taking the following steps immediately after becoming aware of a data breach:

1. **Contain** the breach and minimise any resulting damage, for example asking the incorrect recipient to delete, return, or destroy the information and not read it;
2. **Evaluate** and identify the type of information that has been breached, any Affected Persons, the cause of the breach, and any likely risks of harm;
3. **Notify** Affected Persons of the breach where appropriate (see part 3);
4. **Act** to mitigate risks by taking any additional actions to contain the breach and minimise the damage;
5. **Prevent** recurrences by taking preventative action based on the type and seriousness of the breach. This may include a review of technical or administrative systems and staff procedures, or training;
6. **Report** the breach internally (see part 4), and to the Privacy Commissioner where appropriate (see parts 5 and 6); and
7. **Comply** with the MNDB scheme in relation to any Eligible Data Breach (see part 6).

## 3. Notifying Affected Persons about a data breach

Legal Aid NSW is required under the MNDB scheme to notify Affected Persons about any Eligible Data Breach except where it will cause undue distress or is not reasonably practicable.

Staff will generally also notify an Affected Person about any Other Data Breach. At the same time, we may give them advice about how to deal with the breach to minimise its impact, make a complaint or seek internal review, and outline any actions we will take to help prevent the data breach from happening again.

We may however decide not to tell the Affected Person if the Other Data Breach is minor, or if we think that telling them might cause undue distress or is not reasonably practicable.

## 4. How Legal Aid NSW reports data breaches internally

Staff are required to report a data breach in accordance with the **Roles and Responsibilities** guideline by using the **Data Breach Report Form**, both of which are available to Staff on the intranet. This procedure requires that a data breach is reported to the Privacy Officer in addition to the following:

- Minor Incident: **Supervisor/Solicitor in Charge (SIC)**
- Formal Complaint: **Director**
- Eligible Data Breach or Serious Breach: **CEO**

Further, all data breaches are reported by the Privacy Officer to the Executive twice per year in January and July. This report includes a de-identified summary of each data breach, and the actions taken in response to the breach. An aggregate of the number of data breaches that occur across each reporting period is also reported to the Executive to enable assessment of longer-term data breach trends.

## 5. What does Legal Aid NSW consider to be a Serious Breach?

Even if they are not an Eligible Data Breach, Legal Aid NSW still considers any Other Data Breach to be a Serious Breach where they involve one or more of the following:

- an intentional or malicious breach
- a large volume of personal or health information
- multiple Affected Persons
- a risk of harm to Affected Persons
- an ongoing risk of further data breaches
- media or external interest, or
- a risk of loss or reputational harm to Legal Aid NSW.

## 6. How Legal Aid NSW complies with the MNDB scheme

In compliance with the MNDB under Part 6A of PPIP Act, and except in accordance with any relevant exemption, Legal Aid NSW will take all actions as required under the Act including the following:

- report to the Privacy Officer any suspected Eligible Data Breach
- immediately make all reasonable efforts to contain the data breach
- appoint an assessor, who may or may not be a Legal Aid NSW staff member, but who will not be suspected of being involved in the breach
- within 30 days of becoming aware of the breach, take all reasonable steps to complete an assessment of whether the data breach is an Eligible Data Breach having regard to the Privacy Commissioner Statutory Guidelines and where appropriate using the IPC Self-assessment Tool, and during this time make all reasonable attempts to mitigate the harm done by the suspected breach
- notify the Privacy Commissioner of any extensions of the assessment period, and where requested the progress of the assessment
- If after the assessment, the Privacy Officer decides there is an Eligible Data Breach, immediately notify the Privacy Commissioner using the IPC

Notification Form and notify Affected Persons where reasonably practicable, or if not include a public notification on the Legal Aid NSW website except to the extent it would:

  - Contain personal information;
  - Prejudice Legal Aid NSW functions;
  - Breach sections 25 or 26 of the *Legal Aid Commission Act 1979* (NSW);
  - Breach secrecy provisions in any other Act or statutory rule except for the PPIP Act; or
  - Meet any other relevant exemption under Div 4, Part 6A of the PPIP Act.

- notify the Privacy Commissioner of any further information or exemption
- respond to any Privacy Commissioner directions or recommendations
- establish and maintain an internal register for Eligible Data Breaches, and a public notification register
- update the Privacy Management Plan and relevant policies and procedures; and
- make this Data Breach Policy publicly available on the Legal Aid NSW website.

## 7. Post data breach review

Legal Aid NSW may undertake a review following a data breach as an opportunity to evaluate and strengthen information security and data handling practices to reduce the likelihood of future breaches.

Following a data breach, we may undertake further investigations as to what went wrong, how issues were addressed and whether changes to systems, processes and procedures would mitigate future risks. We may also revise this Policy in light of the outcome of a post data breach review.

## 8. Delegation under the PPIP Act

Pursuant to s 59ZJ of the PPIP Act, the Legal Aid NSW CEO has delegated the exercise of all functions under Part 6A of the Act, other than the power of delegation, to the Manager, In-house Counsel Unit in their capacity as Privacy Officer.

## 9. Contact Details

If a staff member is unsure about anything mentioned in this policy or requires more information about this policy, they can do so by emailing the Privacy Officer at inhousecounselunit@legalaid.nsw.gov.au.

The Data Breach Policy is produced by the Legal Aid NSW In-house Counsel Unit. The Policy may be amended at any time and will be reviewed on a regular basis to ensure ongoing compliance with the Privacy Legislation.