Data Breach Procedure

Version 1.1

August 2025

1 Introduction

This procedure sets out how the NSW State Emergency Service (**NSW SES**) responds to and manages eligible data breaches in line with the Mandatory Notification of Data Breach Scheme (**MNDB Scheme**) established under the *Privacy and Personal Information Protection Act 1998* (**PPIP Act**).

2 Purpose

The NSW SES is committed to ensuring the confidentiality, integrity, and availability of personal information. We protect personal information by taking proactive measures to prevent data breaches. We will respond quickly and effectively when a breach occurs and take action to minimise harm to members of the public and members of our agency.

This procedure provides guidance for members and informs the community of NSW SES practices for managing data breaches involving personal information.

3 Scope and Application

This procedure applies to all staff including third parties engaged to handle personal information on our behalf.

This procedure applies only to data breaches that involve personal information held by NSW SES, which includes personal information:

- in the possession or control of NSW SES or a person employed or engaged by the agency in the course of their employment or engagement, or
- which is contained in a State Record in respect of which the agency is responsible under the *State Records Act 1998*.

Personal information can be ‘jointly held’ by more than one agency or entity.

All third-party contractors are subject to privacy obligations and must handle personal information in line with the PPIP Act. NSW SES must be advised as soon as a contractor becomes aware of a data breach involving personal information being handled on behalf of NSW SES.

Contents

4 What is an 'eligible data breach'?

Under the MNDB Scheme, the NSW SES is required to notify the Privacy Commissioner and affected individuals of an eligible data breach.

For a data breach to constitute an '**eligible data breach**', there are two tests to be satisfied:

1. There is an unauthorised access to, or unauthorised disclosure of, personal information held by NSW SES or there is a loss of personal information held by the agency in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of the information (whether held in digital or hard copy); and
2. A reasonable person would conclude that the access or disclosure of the information would likely result in serious harm to an individual to whom the information relates.

An eligible data breach may include, amongst other things, as follows:

- A cyber-attack resulting in a loss of personal information;
- An email containing sensitive personal information being sent to the wrong recipient;
- The unauthorised release of a beacon report containing personal information of NSW SES members or members of the public; or
- Hard copy documents or notes containing personal information being misplaced.

5 Response to a data breach

5.1 Identification and escalation

All members and third-party providers are responsible for taking immediate, common-sense steps to contain the breach, and must immediately report suspected eligible data breaches to a NSW SES Manager of grade zone 9/10 or above (**Manager**), this must be a NSW SES staff member e.g. Deputy Zone Commander.

The Manager must as soon as practical and **within 1 business day** consider if the breach is potentially an eligible data breach. The flow chart listed at Appendix A and the Information and Privacy Commission NSW (**IPC**)'s *Data Breach Self-assessment Tool* may assist this initial assessment.

At any point the Manager may choose to consult with or seek advice from the Legal team

If it may be an eligible data breach, the Manager must immediately notify the Information and Privacy Officer at gipa@ses.nsw.gov.au or on 0477 367 223.

The Manager must document their decisions in accordance with the *State Records Act 1998.*

5.2 Containment and assessment

Once a suspected eligible data breach is reported it is to be considered by an Assessor appointed by the Commissioner. The NSW SES will immediately make all reasonable efforts to contain the breach and mitigate harm arising from the data breach.

The Assessor will expeditiously and **within 30 calendar days** carry out an assessment of whether the data breach is, or there are reasonable grounds to believe that the data breach is, an eligible data breach. This is in line with the requirements of the MNDB Scheme and relevant guidance issued by the IPC.

The Assessor must consider the *IPC Statutory Guidelines on the assessment of data breaches under Part 6A of the PPIP Act* when assessing a suspected eligible data breach.

If an assessment cannot reasonably be conducted within 30 calendar days (for example if there is a complex cyber-attack and an investigation is still under way), the period to conduct the assessment may be extended by the Commissioner. NSW SES must notify the Privacy Commissioner of any extension.

All data breaches are different and will be assessed on a case-by-case basis. A person suspected to be involved in an action that led to the breach cannot be an Assessor.

5.3 Data Breach Response Team

Depending on the nature and circumstances of the breach, a Data Breach Response Team (**DBRT**) may be formed to conduct a detailed investigation. The DBRT includes representatives appropriate to respond to the breach, including individuals who may be required to further investigate and respond to the breach. These representatives may include Media, Cyber Security, Probity and Standards, the data owner, relevant zone staff etc. The DBRT assists to determine and action any containment steps.

5.4 Notifying an eligible data breach

If a breach is assessed and found to be an eligible data breach, the NSW SES must immediately notify the Privacy Commissioner and notify affected individuals as soon as practicable (unless an exemption applies).

At all times the NSW SES's key priority is to support members of the public and our people, and to mitigate any harm that may arise.

There are some limited exemptions under the MNDB Scheme where the NSW SES may not be required to notify for a breach. For example, the NSW SES will be exempt from notifying where another agency has undertaken to notify for the same breach.

If an exemption is relied upon, the NSW SES must notify the Privacy Commissioner.

5.5 Non-eligible data breaches

There may be circumstances where it may be necessary for the NSW SES to notify under another legislative scheme, or on a voluntary basis.

The NSW SES will notify breaches:

- involving Tax File Numbers that are assessed as meeting the threshold of an 'eligible data breach' under the *Privacy Act 1988* (Cth) to the Office of the Australian Information Commissioner; or

- involving personal information received under the *Data Sharing (Government Sector) Act 2015* to the IPC.

We may also notify individuals on a voluntary basis i.e. where the breach is not likely to result in serious harm to an individual. This will depend on the circumstances of the breach, and may happen:

- to be transparent when something has gone wrong;
- to prevent any immediate and foreseeable harm to the individual; or
- where a member of the public has raised the handling of their personal information by the NSW SES.

Sometimes, notifying individuals of minor breaches can cause undue stress or harm. The NSW SES will also consider any unintended consequences when deciding whether to notify individuals on a voluntary basis.

5.6 Registers

All eligible data breaches will be listed in NSW SES's Internal Register of eligible data breaches. Where it is not possible or reasonably practicable to notify affected individuals directly about the eligible data breach, the NSW SES will notify by placing a public notice on our website and taking reasonable steps to publicise this notification.

6 Roles and Responsibilities

6.1 All NSW SES Members and third party providers

- Be aware of their obligations under the MNDB Scheme.
- Advise a staff manager immediately when they suspect an eligible data breach has occurred.
- Act on any advice from their Manager and the Legal team or the DBRT to contain the breach.

6.2 Legal team

- Responsible for privacy management across NSW SES.
- Coordinate response and activation of DBRT if required.
- Provide specialist advice and assistance when a suspected eligible data breach occurs.
- Report the data breach to the NSW SES Commissioner.
- Report the breach to the Information Privacy Commissioner if required.
- Notify effected individuals if required.
- Update and maintain registers and facilitate public notices if required.

6.3 Data Breach Response Team

- The purpose of a DBRT is to respond to complex or higher risk breaches.
- Conduct initial assessment of breach and determine if response is required.
- The DBRT is made up of those people within NSW SES who are best placed to investigate and respond.

6.4 NSW SES Commissioner

- Where a breach occurs, ensure the agency has:
  - made all reasonable efforts to contain the data breach; and
  - expeditiously and within 30 days of becoming aware of the breach, carried out an assessment and determined if it is an eligible breach,

  in line with the MNDB Scheme.
- Where a breach or suspected breach occurs, ensure the agency has made all reasonable attempts to mitigate harm in line with the MNDB Scheme.

7 Related Documents

- NSW SES Code of Conduct and Ethics
- *Government Information (Public Access) Act 2009*
- *Privacy and Personal Information Protection Act 1998*
- *Health Records Information Privacy Act 2002*
- *State Records Act 1998*
- Privacy Management Plan
- Cyber Security Policy
- Information Classification, Labelling and Handling Guideline
- Information Governance and Management Framework

8 Support and Advice

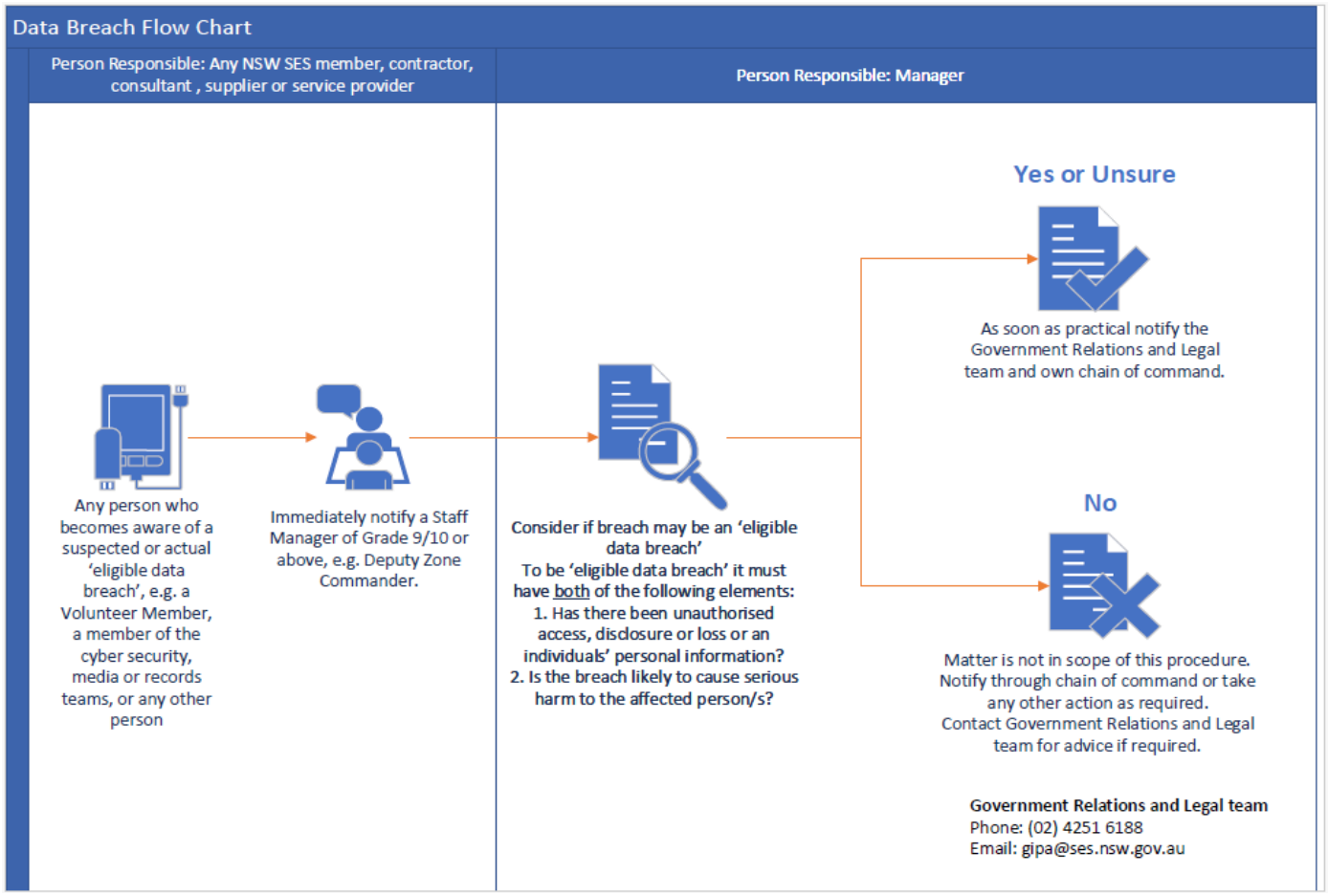
You can get advice and support about anything in these procedures from:

- your manager or zone staff
- the Policy Owner – ManagerLegal
- the Policy Sponsor – Chief of Staff
- by emailing gipa@ses.nsw.gov.au
- by calling (02) 4251 6188

9 Definitions

Term	Definition
Assessor	This is one of the following: • A member of the Legal team; • Chief of Staff; or • A third party contractor who is engaged to act on behalf of NSW SES.
IPC	The Information and Privacy Commission NSW.
Member	This includes volunteers, staff (ongoing, temporary and agency), contractors and consultants.
Manager	A NSW SES staff member employed or acting at Grade 9/10 or above
Personal information	The references to personal information in this procedure has the same meaning as section 4 of the PPIP Act and includes health information within the meaning of the *Health Records and Information Privacy Act 2002*. Personal information includes information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. For example, a person's name, contact details, address or images of the person will be considered personal information.
Eligible data breach	Has the same definition as set out in the PPIP Act (as updated from time to time).

Appendix A – Identification of 'eligible data breach' process flowchart



Document Control Sheet

Title	Data Breach Procedure
Current Version #	1.1
Document Hierarchy	Cyber Security Policy
Directorate	Office of the Commissioner
Procedure Owner	Manager Legal
Procedure Sponsor	Chief of Staff
Effective date	06/04/2024
Next Review Date	06/04/2027
Rescinds	Data Breach Procedure v1.0
Topic	Compliance
Function	Governance
Key Words	Data breach, Eligible data breach, Mandatory Notification of Data Breach

Version History

Version #	Creation Date	Author	Summary of changes
1.0	05/03/2024	Geoff James	Creation of procedure
1.1	28/08/2025	Manager Legal	Owner and contact details updated to Manager Legal.

Approval

Title		Date	Version signed off
Manager Legal	Procedure Owner	28/08/2025	1.1
Chief of Staff	Procedure Sponsor	05/03/2024	1.0
Commissioner	Commissioner	06/04/2024	1.0