# Data Breach Policy

## Audit and Assurance Unit
## Business Coordination, Compliance and Reporting

Document ID: CG03-015

Version: 1
Issued: 7 August 2025

# Contents

# 1 Introduction

**This policy is intended to advise FRNSW staff, including firefighters, volunteers and contractors, and the community of NSW of the obligations that FRNSW has in relation to protecting the privacy of their personal and health information.**

**This policy establishes the actions required of FRNSW when it becomes aware of a data breach under the Privacy and Personal Information Protection Act 1998, and other laws relating to keeping personal information secure.**

## 1.1 Background and purpose

Fire and Rescue NSW (FRNSW) is committed to managing Personal and Health Information in accordance with its obligations under the:

- *Privacy and Personal Information Protection Act 1998* (NSW) (**PPIP Act**), including the Information Protection Principles (**IPPs**);
- *Health Records and Information Privacy Act 2002* (NSW) (**HRIP Act**), including the Health Privacy Principles (**HPPs**); and
- *Privacy Act 1988* (Cth) (**Privacy Act**), including the Australian Privacy Principles (**APPs**),

as well as other applicable legislation and guidelines, to protect all Personal and Health Information that it collects, uses and shares (collectively '**Privacy Laws'**), including the NSW Government Information Classification, Labelling and Handling Guidelines.

## 1.2 NSW Mandatory Notification Data Breach Scheme for FRNSW

From 28 November 2023, amendments to the PPIP Act which establish the NSW Mandatory Notification Data Breach Scheme (**NSW MNDB Scheme**) come into effect.

Under the NSW MNDB Scheme, FRNSW is required to prepare and publish a Data Breach Policy (**DBP**) for managing eligible data breaches. Please refer to Section 4.2 for further guidance.

This DBP sets out the processes that all FRNSW Personnel and other parties to which this DBP applies must follow in the event of a data breach or Eligible Data Breach (as defined in Section 4.2). In particular, this DBP sets out:

- the steps FRNSW has taken to prepare for a data breach;
- the steps to be taken in the event that an actual or suspected data breach or Eligible Data Breach occurs; and
- the roles and responsibilities of FRNSW Personnel and other parties to which this DBP applies.

## 1.3 Commonwealth NBD Scheme

In addition to its notification obligations under the PPIP Act and HRIP Act, FRNSW has also notification obligations under the Federal Privacy Act. Please refer to Section 4.2 for further guidance.

### 1.4 1.5 This DBP and our Data Breach response strategy

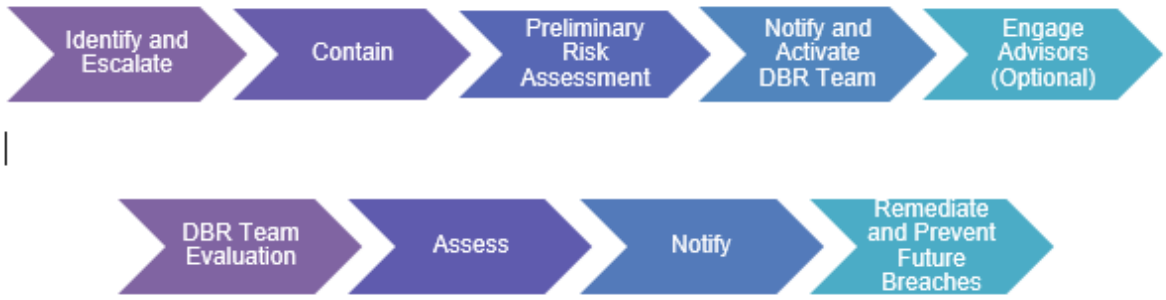
This DBP is intended to:

► enable FRNSW to meet its obligations under the Privacy Laws;

► provide all staff, including firefighters, administrative and trades staff, volunteers, contractors, consultants and skill hire staff of FRNSW (collectively, **Personnel**), and external entities including Suppliers and their personnel who access Personal, and Health Information collected by FRNSW with guidance on what a data breach is and how / where to report it; and

► instil confidence in the community and FRNSW's key stakeholders regarding our ability to protect Personal and Health Information and to appropriately respond to data breaches (including Eligible Data Breaches).

FRNSW's data breach response strategy is outlined in the below diagram.




## 2 Preparation for Data Breaches

This section outlines the steps that FRNSW has taken to prepare for a data breach, as well as how the management of data breaches fits in with FRNSW's broader policy framework.

### 2.1 Training and Awareness

FRNSW promotes awareness of privacy obligations among Personnel and third parties by:

► publishing this DBP and FRNSW's privacy-related policies on FRNSW's intranet and website;

► publishing information about privacy on FRNSW's intranet;

► communicating regularly with Personnel and third parties about privacy;

► ensuring FRNSW Personnel and third parties are aware of their privacy obligations;

► ensuring FRNSW policies comply with privacy laws;

► requiring privacy training as part of the induction process; and

► providing training and advice to Personnel and third parties (both at induction and on an ongoing basis), including a mandatory privacy awareness training

### 2.2 Policy Framework

The following internal FRNSW policies and procedures contain individual references to enable Personnel to manage Personal and Health Information collected for different purposes:

- Privacy Policy;
- Privacy Management Plan;
- Code of Conduct and Ethics;
- eAIRS Data Management policy and procedures;
- Data Management Policy;
- In Orders 2006/13, Overt video surveillance policy;
- In Orders 2006/11, Recording of radio, telephone and paging messages;
- In Orders 1990/4, Access to Communication Centre information;
- In Orders 1998/25, Incident notebooks; and
- Public Interest Disclosures Policy.

# 3 How to identify Data breaches

## 3.1 What is a Data Breach?

Data breaches can arise in several ways but typically fall into one of the following categories:

| | |
|---|---|
| **Data is accessed by someone who is not authorised to access the information** | Personal and Health Information (which may also include Sensitive Information (as defined below in section 3.2) and/or TFN Information (as defined below in section 3.4)) is accessed, visible or retrievable by people (including Personnel) who are not authorised to access, view or retrieve the information. |
| **Data is shared with someone who is not authorised to access the information** | FRNSW makes Personal and Health Information (which may also include Sensitive Information and/or TFN Information) accessible, visible, or retrievable by people within or outside FRNSW who are not authorised to see it. This could include:<br>▪ FRNSW Personnel sending an email containing personal information to the wrong recipient; or<br>▪ information has been obtained via a malicious actor emailing / phoning FRNSW and impersonating another individual to obtain personal information of the impersonated individual from FRNSW Personnel. |
| **Data is lost (e.g., the whereabouts of some information is no longer known, or information cannot be retrieved)** | Personal and Health Information (which may also include Sensitive Information and/or TFN Information) is contained in paper or digital form and the paper document or storage device is lost / cannot be located. This could include:<br>▪ leaving a work mobile, laptop, or other device behind on the train or in a cafe; |

| | |
|---|---|
| | ▪ inadvertent deletion of destruction of Personal and Health Information. |
| **Data is unable to be accessed (e.g., data being hacked and/or held ransom)** | This includes any scenario when FRNSW is unable to access Personal and Health Information (which may also include Sensitive Information and/or TFN Information), including as a result of a systems outage, data ransom or other cyberattack that results in information being inaccessible. |

## 3.2 What is Personal Information?

For FRNSW, Personal Information is defined in section 4 of the PPIP Act. In summary, Personal Information is information or an opinion about an individual whose identity is apparent or could be reasonably determined.

Exclusions as to what constitutes Personal Information can be found at subsections 4(3) and 4A of the PPIP Act.

For more information as to what information constitutes Personal Information, or any applicable exclusions refer to section 4 and subsections 4(3) and 4A of the PPIP Act or contact the Privacy Contact Officer.

The PPIP Act also includes special restrictions on the disclosure of Personal Information that is also Sensitive Information (being information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities).

## 3.3 What is Health Information?

For FRNSW, Health Information is defined in section 6 of the HRIP Act as, subject to some inclusions, being a subset of Personal Information. Under the HRIP Act, Health Information includes Personal Information that is also information or an opinion about a person's physical or mental health or disability, information connected to the provision of a health service or genetic information that is or could be predictive of the health of a person or their relatives or descendants.

Exclusions as to what constitutes Health Information pursuant to the HRIP Act can be found at section 6 of the HRIP Act.

For more information on these exclusions, refer to section 6 of the HRIP Act or contact the FRNSW Privacy Contact Officer at privacyofficer@fire.nsw.gov.au

## 3.4 Compliance with the TFN Rule

FRNSW must comply with the requirements for the handling of TFNs, as imposed by the "TFN Rule", contained within the Privacy (Tax File Number) Rule 2015 (Cth), passed pursuant to section 17 of the Privacy Act.

Pursuant to the TFN Rule, FRNSW must not record, collect, use or disclose a staff member's Tax file number information unless expressly permitted to under taxation, personal assistance or superannuation law.

Tax file number information is defined in section 6 the Privacy Act as "information, whether compiled lawfully or unlawfully, and whether recorded in a material form or not, that records the tax file number of a person in a manner connecting it with the person's identity" (**TFN Information**).

# 4 Mandatory Reporting of Data Breaches

## 4.1 Mandatory Notification of an Eligible Data Breach for FRNSW

*Commonwealth NDB Scheme*

The Privacy Act establishes the Commonwealth Notifiable Data Breaches scheme (**Cth NDB Scheme**), which requires organisations covered by the Privacy Act to notify individuals likely to be at risk of serious harm due to a data breach. While the Privacy Act primarily regulates Commonwealth government and private sector agencies, the Privacy Act also contains provisions that apply to public sector agencies in relation to data breaches involving TFNs.

A data breach will be classified as an '**Eligible Data Breach'** (also referred to as "notifiable data breaches") for the purposes of the Commonwealth NDB Scheme where:

- there is unauthorised access to or unauthorised disclosure of, the information and a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates; or
- the information is lost in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and assuming that 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 any of the individuals to whom the information relates.

For the avoidance of doubt, any breach relating to TFN Information is to be treated as an Eligible Data Breach.

*NSW MNDB Scheme*

From 28 November 2023, amendments to the PPIP Act will establish the NSW MNDB Scheme. The NSW MNDB Scheme will require organisations covered by the PPIP Act (including FRNSW) to notify the IPC where individuals are likely to be at risk of serious harm due to a data breach.

A data breach will be classified as an '**Eligible Data Breach'** for the purposes of the NSW MNDB Scheme where:

- the unauthorised access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the Personal and Health Information relates. These breaches are also commonly referred to as 'notifiable data breaches'; and
- a reasonable person would conclude that the access, disclosure or loss is likely to result in serious harm[1] to any of the individuals to whom the Personal and Health Information relates.

The PPIP Act includes the following list of factors that may be considered when assessing the severity of the breach:

[1] *'Serious harm' is not defined in the Privacy Act, however, may include serious physical, psychological, emotional, financial, or reputational harm. OAIC guidance as to what constitutes serious harm (and if serious harm is likely to occur) can be found here.*

- the types of personal information involved in the breach.
- the sensitivity of the personal information involved in the breach.
- whether the personal information is or was protected by security measures,
- the persons to whom the unauthorised access to, or unauthorised disclosure of, the personal information involved in the breach was, or could be, made or given.
- the likelihood of malicious intent by the person who had unauthorised access or disclosure.
- the nature of the harm that has occurred or may occur.
- other matters specified in guidelines issued by the Privacy Commissioner about whether the disclosure is likely to result in serious harm to an individual to whom the personal information relates.

To avoid doubt, an Eligible Data Breach may include the following:

- a data breach that occurs within a public sector agency;
- a data breach that occurs between public sector agencies; and
- a data breach that occurs by an external person or entity accessing data held by a public sector agency without authorisation.

Any breach relating to TFN Information is an Eligible Data Breach.

*Notification of Eligible Data Breaches*

Eligible Data Breaches **must** be notified to the following parties:

1. for Eligible Data Breaches involving TFNs, to:
    a. the Office of the Australian Information Commissioner (**OAIC**) as soon as practicable. This should be done using the Notifiable Data Breach Form.
    b. to the IPC immediately unless otherwise authorised by the relevant member of the Executive Leadership Team (**ELT**).
2. for Eligible Data Breaches which will be covered by the NSW MNDB Scheme once it comes into effect on 28 November 2023 following amendments to the PPIP Act, to the IPC immediately;
    a. for Eligible Data Breaches other than those referenced in point 1 above, to the IPC immediately.
3. each affected individual as soon as practicable;
4. each individual to whom the personal information the subject of the breach relates as soon as practicable; and
5. other third parties (including other regulators, suppliers or customers).

## 4.2 Other Data Breach Notification Schemes

Further to the Commonwealth NDB Scheme and the NSW Voluntary Reporting Scheme/NSW MNDB Scheme, FRNSW also has obligations under the following data breach notification schemes in certain circumstances. Data breaches arising from the following circumstances must be reported, for data breaches in respect of information received by the government sector agency (**Data Recipient**) under the *Data Sharing (Government Sector) Act 2015* (NSW) (**DSGS Act**) to the IPC and the government sector agency that controls Privacy.

# 5 Document Review

## 5.1 Document control

| | |
|---|---|
| **Policy Manager** | Manager Audit & Assurance |
| **Contact Officer** | Privacy Contact Officer |
| **Contact No** | +61 2 9269 6451 |
| **Document type** | Policy |
| **Applies to** | ☑ Firefighters<br>☑ Community Fire Unit Members<br>☑ Administrative and Trades Staff<br>☑ Contractors and Consultants |
| **Status** | Draft |
| **Security** | Official |
| **File Reference** | FRN23/3471 |
| **Review Date** | Three years from date of publication |
| **Rescinds** | New document |
| **Copyright** | © State of New South Wales through Fire and Rescue NSW |
| **Version approved by** | Commissioner |
| **Date approved** | 7 August 2025 |
| **Approval File Reference** | APP25/720 |

## 5.2 Revision history

| Version | Date | Status | HPE RM Ref | Details |
|---|---|---|---|---|
| 01 | 20/05/2025 | Final | FRN23/3471 | New policy |