NSW Police Force

NSW Police Force Data Breach Policy

Infolink, Communication Services Command

NSW Police Force: Data Breach Policy

The NSW Police Force (NSWPF) takes its obligations to have reasonable security safeguards and mechanisms in place to protect personal and health information seriously. This Data Breach Policy (this Policy) explains how we fulfill our obligations under NSW privacy laws to notify a breach of personal and health information, should such a breach occur.

Effective privacy and data breach management underpins this obligation and assist us to prevent incidents and avoid or reduce potential harm to affected individuals.

Essential Summary

Personal and health information that is collected, stored, and used by the NSW Police Force (NSWPF) must be protected appropriately throughout its lifecycle to ensure its security, confidentiality and integrity. This Policy provides a framework for the NSWPF's compliance with the Mandatory Notification of Data Breach Scheme (the MNDB Scheme).

This Policy provides guidance on the following topics:

- the MNDB Scheme and its obligations
- the definition of an eligible data breach
- how the NSWPF responds to an eligible breach
- the roles and responsibilities of NSWPF staff
- how the NSWPF notifies affected individuals in the event of an eligible data breach
- how the NSWPF conducts Post Incident Reviews
- how the NSWPF maintains its public register
- the obligations of NSWPF private sector providers.

Document Control Sheet

Document Properties

Title	Data Breach Policy
Subject	To outline how the NSW Police Force will prevent and mitigate privacy and data breaches
Command responsible	Infolink, Communication Services Command
Authorisation	Commissioner of Police, NSW Police Force
Security Classification / Information Management Markings	Unrestricted
Publication date	November 2023
Current version number	1.0
Review date	November 2024
Document number	D/2023/1333348
Copyright statement	© Crown in right of NSW through NSW Police Force 2023
Suitable for Public Disclosure	YES

Modification History

Version #	Version / approval date	Author/Position	Summary of changes
1.0	November 2023	Privacy Manager	Creation of document

Table of Contents

1. Introduction

1.1. Purpose

The purpose of this Policy is to provide an overview of the NSWPF's procedures in relation to containing, assessing, managing, notifying and reporting on eligible data breaches in accordance with the Mandatory Notification of Data Breach Scheme (the MNDB Scheme).

The MNDB Scheme commenced on 28 November 2023 as part of recent amendments under Part 6A of the Privacy and Personal Information Protection Act 1998 (the PPIP Act). The amendments require all public sector agencies, including the NSWPF, to take various steps to contain, assess, manage, notify and report eligible data breaches. This Policy complies with section 59ZD of the PPIP Act.

Notifying individuals affected by a privacy or data breach can enable them to take steps to mitigate the consequences of a breach. It is also a positive step that the NSWPF can take to help rebuild trust with the affected individuals. Additionally, the MNDB Scheme requires NSWPF to also notify eligible breaches to the NSW Privacy Commissioner, allowing for independent advice, assessment and investigation of a breach.

1.2. Scope

This Policy applies to:

- all NSWPF permanent full time, part time, trainee and temporary employees (which, for the avoidance of doubt, includes including all sworn and unsworn members of the NSWPF) and approved users of NSWPF information systems and assets
- any person or organisation authorised to administer, develop, manage and support NSWPF information systems and assets
- third party suppliers, vendors, contingent labour contractors, and hosted/managed service providers.

2. Privacy and data breaches

2.1. What is an eligible data breach?

Under the MNDB Scheme, an eligible data breach occurs where:

- there is 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
- 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.

2.2. Types of data breaches

Examples of data breaches may include (but are not limited to):

Human error

- Letter or email is sent to the wrong recipient
- System access incorrectly granted to someone without authorisation
- Physical assets are lost or misplaced, such as paper records, USBs or laptops.

Systems failure

- Coding errors allowing system access without authentication or automatic notice generation
- Failure to apply known and supported patches to software.

Malicious or criminal attack

- Cyber incidents such as ransomware, malware, hacking, phishing or brute force access attempts
- Social engineering and impersonation attempts
- Insider threats (employees) using valid credentials to access or disclose personal information outside the scope of their duties or permissions.

2.3. What is serious harm?

Whether a data breach is likely to result in serious harm requires an objective assessment, determined from the viewpoint of a reasonable person. Serious harm occurs where the incident may result in a real and substantial detrimental effect on an individual (the effect must be greater than irritation, annoyance or inconvenience).

Types of serious harm that may occur as a result of an eligible data breach may include physical, emotional, psychological, financial or reputational harm to an individual.

The potential harm that can arise as a result of a data breach is context-specific and will vary based on the:

- type of information accessed, disclosed or lost and whether a combination of types of information might lead to increased risk
- level of sensitivity of the information accessed, disclosed or lost
- amount of time the information was exposed or accessible, including prior to the discovery of the breach
- circumstances of the individuals affected and their vulnerability and susceptibility to harm
- circumstances in which the breach occurred
- actions taken by the NSWPF to reduce the risk of harm following a breach.

3. Responding to a data breach

3.1. Key steps in responding to an eligible breach

The four steps to respond to a data breach are:

1. **Report** and **contain** the impact of the breach
2. **Assess** the breach and its risks
3. **Notify** the Privacy Commissioner and affected individuals as required
4. **Review** and **report** on the breach

The NSWPF maintains an internal *Data Breach Response Plan*, which sets out the roles and responsibilities for managing the response to a data breach

3.2. Roles and responsibilities

The NSWPF has assigned different responsibilities to certain roles within our organisation:

Head of Agency/Assessor

The Head of Agency has delegated responsibilities to the following roles within the NSWPF.

All NSWPF employees

All NSWPF employees must report to their immediate supervisor or manager if they have reasonable grounds to suspect there may have been a privacy or data breach, who will report the suspected breach to the Professional Standards Duty Officer or other delegate authorised to receive reports of suspected data breaches. All NSWPF employees must also make all reasonable efforts to contain a suspected breach and mitigate the harm done.

Professional Standards Duty Officers and Professional Standards Managers

For Police Area Commands/Districts and Business Units, the Professional Standards Duty Officer or other nominated Manager has primary responsibility for identifying whether a suspected breach is an eligible breach or not and preparing an internal notification. In the event of a suspected eligible breach, the Privacy Manager may direct the Professional Standards Manager to conduct an assessment in accordance with the requirements of the MNDB Scheme to confirm that the breach is an eligible breach.

Privacy Manager

The Privacy Manager receives internal notifications from Professional Standards Duty Officers or equivalent Managers/Inspectors on suspected eligible data breaches and directs Professional Standards Managers to conduct assessments to confirm if a suspected data breach is an eligible data breach. The Privacy Manager may provide advice to the Professional Standards Manager and may decide that a Data Breach Response Team is required. The Privacy Manager is also responsible for notifying the Privacy Commissioner of eligible breaches, maintaining registers and reports and

updating policies and plans as required. The Privacy Manager also provides advice and training to all NSWPF employees on their privacy obligations under the MNDB Scheme.

Data Breach Response Team

A Data Breach Response Team (the Response Team) may be convened by the Privacy Manager to respond to complex data breaches. The Response Team is constituted in accordance with the NSWPF Data Breach Response Plan and can be scaled depending on the size of the data breach, the resources required to respond, and the number of agencies affected.

It may contain employees from within the NSWPF across relevant areas such as Legal, Information Security, Cyber and Public Affairs, as well as other agencies or contractors where specialist services are required to respond to a breach.

3.3. Notification of affected individuals

Affected individuals will be notified as soon as reasonably practicable with the following information (if known):

- the date the data breach occurred
- a description of the data breach
- how the data breach occurred
- the type of data breach that occurred
- the personal information that was the subject of the breach
- the amount of time the personal information was disclosed for
- actions that have been taken or are planned to ensure the personal information is secure, or to control or mitigate the harm done to the individual
- recommendations about the steps the individual should take in response to the data breach
- information about the making of privacy related complaints and internal reviews under the PPIP Act
- the name of the public sector agency which was the subject of the data breach
- if more than one public sector agency was the subject of the data breach – the name of each agency
- contact details for a person nominated by the agency for the individual to contact in relation to the breach.

We may not notify affected individuals in certain circumstances, including:

- where multiple agencies are involved in an eligible breach and one of those agencies has provided notification
- where an eligible data breach would prejudice an ongoing investigation and certain proceedings

- where the NSWPF has taken action before the data breach results in serious harm or loss to individuals
- where compliance would be inconsistent with secrecy provisions in other legislation
- where compliance would result in serious risk of harm to the health and safety of an individual
- where compliance would worsen the NSWPF's cyber security or lead to further data breaches.

Affected individuals should be notified, however if it is not reasonably practicable to identify or notify the individuals (for example, due to the size of the breach or the fact specific individuals and/or their contact details cannot be determined), the NSWPF will, if reasonably practicable, publish a notification on the NSWPF website.

3.4. Post-breach review and evaluation

Following an eligible data breach, the Privacy Manager or Data Breach Response Team conducts a Post Incident Review.

A Post Incident Review provides an opportunity for the NSWPF to learn from an eligible data breach and to improve its practices, procedures, systems, information handling practices, information security measures and to eliminate and reduce the chance of reoccurrence.

A Post Incident Review may include the following:

- examining the cause of the breach, including identifying any weaknesses in information handling and/or systems/technology that gave rise to the breach
- consideration of whether the breach was a systemic problem or an isolated incident
- reviewing and improving physical and environmental security requirements, including auditing requirements
- assessing IT systems for vulnerabilities and taking preventative measures to negate the risk of a data breach reoccurrence
- making appropriate changes to NSWPF policies, procedures and, where appropriate, contracts including updating this Policy and corresponding policies
- identifying further learning and training opportunities
- gathering feedback from key stakeholders engaged in responding to the breach to identify lessons learned from the breach response.

3.5. Registers and reporting

The Privacy Manager coordinates record keeping for each data breach, including maintenance of the internal NSWPF Data Breach Register. Information about every data breach is recorded, regardless of whether the breach amounts to an eligible breach or not under the MNDB Scheme.

The NSWPF also maintains a public notification register on the NSWPF website. This is used to provide public notifications of eligible data breaches where NSWPF is unable to notify, or it is not reasonably practicable to notify, affected individuals.

3.6. Breaches involving private sector providers

The NSWPF works with private sector providers to facilitate a range of services.

The MNDB Scheme does not generally apply to private sector service providers providing services on behalf of government. This is because information held by a private sector service provider is usually 'held' by the service provider and not by a public sector agency.

However, information in the hands of a private sector service provider may still be 'held' by the NSWPF if the NSWPF is in 'possession or control' of the information, for example if the agency retains a legal or practical power to deal with the personal information – whether or not the NSWPF physically possesses or owns the medium on which the personal information is stored.

Under this Policy, all NSWPF service providers are required to promptly report data breaches to the NSWPF and assist the NSWPF in undertaking data breach assessments and its other functions under the MNDB Scheme.

4. Related legislation and policies

This Policy supports adherence to:

- *Privacy and Personal Information Protection Act 1998*
- *Health Records and Information Privacy Act 2002*
- *State Records Act 1998*

This Policy is supported by:

- *NSWPF Privacy Management Plan*
- *NSWPF Data Breach Response Plan*
- *NSW IPC MNDB Scheme Resources Page*
- *NSW Cyber Security Policy*
- *Information management and technology policies on the NSWPF Intranet*
- *NSWPF Cyber Incident Response Plan*