Office of the Inspector of the Independent Commission Against Corruption

Data Breach Policy

January 2024

NSW GOVERNMENT

Document management

Publication details

Document type(s) (select all that apply)	Yes/No
Policy	Yes
Procedures	Yes
Guidelines	No
Standard	No
Fact sheet	No

Publication (select all that apply)	Yes/No
Not for publication	No
Inspector's website	Yes

Approved by	Date of approval
Inspector of the Independent Commission Against Corruption	15 January 2024

Review record

Date	Action	Version
15 January 2024	Policy approved	1
22 January 2024	Updated roles and responsibilities	1.1

Contents

1 Introduction

Part 6A of the *Privacy and Personal Information Protection Act 1998* (NSW) (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'. Under the scheme, public sector agencies are required to prepare and publish a Data Breach Policy (DBP) for managing such breaches as well as maintaining an internal register and public register of eligible data breaches.

This policy draws heavily from the NSW Information and Privacy Commission's (IPC) Data Breach Policy October 2023 and its other online resources for agencies. The IPC's material is gratefully acknowledged.

2 Scope and purpose

This policy provides guidance to the Inspector's staff on data breaches of personal information held by the Inspector in accordance with the requirements of the PPIP Act.

This policy outlines the Inspector's approach to complying with the MNDB scheme, the roles and responsibilities for reporting data breaches and strategies for containing, assessing and managing eligible data breaches.

This policy applies to all staff of the Inspector. It sets out how staff will respond to data breaches involving personal information, bearing in mind that not all data breaches will be eligible data breaches.

The Inspector's Data Breach Response Plan sets out the detailed procedure for managing and responding to data breaches and should also be referred to in the event of a data breach.

It is noted that the Inspector's staff are employed by the Premier's Department to assist the Inspector to perform their functions. Should those staff become aware of a suspected data breach or cyber security incident affecting information held by The Cabinet Office (TCO) or Premier's Department (PD) that does not concern a record that the Inspector holds, The Cabinet Office and Premier's Department Data Breach Policy should be followed.

Where a data breach is also a cyber security incident, the PD/TCO Cyber Incident Response Plan and related procedures will also apply.

3 Definitions

Assessor means a person directed by the Inspector or their delegate to carry out an assessment of a data breach.[1]

Cyber Incident Response Team means a team consisting of PD/TCO staff assembled to coordinate the Inspector's response to a cyber security incident (whether an eligible data breach or not).

Cyber security incident means an occurrence or activity that may threaten the confidentiality, integrity or availability of a system or the information stored, processed or communicated by it.

[1] See s 59G PPIP Act.

Data breach means the unauthorised access to, unauthorised disclosure of, or a loss of personal information held by the Inspector.

Eligible data breach means a data breach likely to result in serious harm to individuals whose personal information is involved in the data breach.[2]

Employee or staff means all PD and TCO employees (ongoing, temporary and casual, and those on secondment to the PD or TCO); contractors (including employees, agents or subcontractors engaged by a contractor) and agency staff engaged to perform work for, or provide services on behalf of, the PD or TCO; work experience students; and volunteers and consultants where their engagement requires adherence to the Premier's Department Code of Conduct who have been engaged specifically for the purpose of supporting the Inspector of the Independent Commission Against Corruption to perform their functions.

Held – personal information is held by the Inspector if:

a. the Inspector is in possession or control of the information, or

b. the information is contained in a state record in respect of which the Inspector is responsible under the *State Records Act 1998*[3]

HRIP Act means the *Health Records and Information Privacy Act 2002* (NSW)

Inspector means Inspector of the Independent Commission Against Corruption

Personal information means information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. In this policy, personal information also encompasses health information within the meaning of the HRIP Act and includes information about an individual's physical or mental health, or disability, or information connected to the provision of a health service to an individual.

PPIP Act means the *Privacy and Personal Information Protection Act 1988* (NSW)

4 Roles and responsibilities

The **Inspector** is responsible for:

- implementing this Policy and all notifications and actions for eligible data breaches
- investigating data breaches, preparing the Data Breach Response Action Plan and maintaining the internal and public registers for data breaches
- immediately reporting all data breaches that are also cyber security incidents to the PD Chief Information Security Officer and/or Chief Digital & Information Officer, if they have not already been reported
- liaising with the **Director, Information and Privacy – Legal Branch, TCO** in relation to a breach or suspected breach where there may be application of The Cabinet Office and Premier's Department Data Breach Policy *and* the Inspector's Data Breach Policy
- communication with affected individuals and external reporting agencies, including notifying the Privacy Commissioner
- complying with their legislative obligations as agency heads in relation to data breaches, including under the PPIP Act.

[2] See s 59D PPIP Act.

[3] s 59C PPIP Act.

The **PD's Chief Information Security Officer** and **Chief Digital & Information Officer** are responsible for:

- immediately reporting all cyber security incidents that are also data breaches concerning information contained in a record held by the Inspector to the Inspector (if they have not already been reported)
- implementing a Cyber Incident Response Plan and related procedures if the data breach is also a cyber security incident
- consulting with the Inspector in respect of how implementation of a Cyber Incident Response Plan and related procedures impacts records held by the Inspector, and
- assembling a **Cyber Incident Response Team** for any data breach that is also a cyber security incident. The Cyber Incident Response Team will manage and provide advice to the Inspector or their delegate in relation to the data breach response.

All staff are responsible for:

- ensuring they have read this policy and the Data Breach Response Plan and that they understand what is expected of them
- immediately reporting a suspected data breach in accordance with this policy
- responding to requests for information from and cooperating with the Inspector, the Chief Information Security Officer, Chief Digital & Information Officer or an assessor appointed to assess a data breach
- otherwise complying with the policy and the Data Breach Response Plan.

5 What is an eligible data breach?

The definition of personal information for the purposes of the MNDB Scheme includes both 'personal information' as defined in section 4 of the PPIP Act and 'health information', as defined in section 6 of the *Health Records and Information Privacy Act 2002* (HRIP Act). This means that for the purposes of the MNDB Scheme, 'personal information' means information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion and includes information about an individual's physical or mental health, disability, and information connected to the provision of a health service.

A data breach occurs when personal information held by an agency (whether held in digital or hard copy) is subject to unauthorised access, unauthorised disclosure or is lost in circumstances where the loss is likely to result in unauthorised access or unauthorised disclosure.

This may or may not involve disclosure of personal information external to the agency or publicly. For example, unauthorised access to personal information by an agency employee, or unauthorised sharing of personal information between teams within an agency may amount to a data breach.

A data breach may occur as the result of malicious action, systems failure, or human error. A data breach may also occur because of a misconception about whether a particular act or practice is permitted under the Information Protection Principles (IPPs).

Examples of causes of data breaches include:

- Human error
  - 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 or misplaced

  - when staff fail to implement appropriate password security, for example not securing passwords or sharing password and log in information
- System failure
  - where a coding error allows access to a system without authentication
  - where a coding error results in automatically generated notices including the wrong information or being sent to incorrect recipients
  - where systems are not maintained through the application of known and supported patches
  - disclosure of personal information to a scammer as a result of inadequate identity verification procedures
- Malicious or criminal attack
  - cyber incidents such as ransomware, malware, hacking, phishing or brute force access attempts resulting in access to or theft of personal information
  - social engineering or impersonation leading into inappropriate disclosure of personal information
  - insider threats from agency employees using their valid credentials to access or disclose personal information outside the scope of their duties or permissions
  - theft of a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information.

The MNDB Scheme applies where an 'eligible data breach' has occurred. There are **two tests to be satisfied** for a data breach to be an 'eligible data breach':

1. there is an 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**
2. 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.

The term 'serious harm' is not defined in the PPIP Act. Harms that can arise because of a data breach are context-specific and vary based on:

- the type of personal information accessed, disclosed or lost, and whether a combination of types of personal information might lead to increased risk
- the level of sensitivity of the personal information accessed, disclosed or lost
- the amount of time the information was exposed or accessible, including the amount of time information was exposed prior to the agency discovering the breach
- the circumstances of the individuals affected and their vulnerability or susceptibility to harm (that is, if any individuals are at heightened risk of harm or have decreased capacity to protect themselves from harm)
- the circumstances in which the breach occurred, and
- actions taken by the agency to reduce the risk of harm following the breach.

Serious harm occurs where the harm arising from the eligible data breach has, or may, result in a real and substantial detrimental effect to the individual. The effect on the individual must be more than mere irritation, annoyance or inconvenience.

Harm to an individual includes physical harm; economic, financial or material harm; emotional or psychological harm; reputational harm; and other forms of serious harm that a reasonable person in the agency's position would identify as a possible outcome of the data breach.

6 Systems and processes for managing data breaches

The Inspector's IT network and infrastructure is managed by the PD and Department of Customer Service (DCS) who have implemented a number of cyber security measures to mitigate the risk of data breaches. This has included projects to increase cyber security maturity, cyber security training for all staff, Data Loss Prevention, and procedures for the storage of personal and sensitive information.

The Inspector will maintain an internal register of data breaches and will implement changes to systems and policies in response to the causes of data breaches in an effort to prevent future breaches.

7 Reporting and responding to a data breach

The Inspector must be informed of **any** data breach to ensure application of this policy, including making notifications to the Privacy Commissioner for eligible data breaches and affected individuals.

There are 5 key steps required in responding to a data breach:

1. Initial report and triage.
2. Contain the breach.
3. Assess and mitigate.
4. Notify.
5. Review.

Each step is set out in further detail below. The first four steps should be carried out concurrently where possible. The last step is concerned with making recommendations for longer-term solutions and prevention.

The Inspector or their nominee will coordinate with PD and DCS and/or its service providers to address and respond to identified data breaches related to its IT systems.

7.1 Step one: initial report and triage

A staff member, contractor or third-party provider is to notify the Inspector within **one business day** of becoming aware that a data breach has occurred and provide information about the breach including as far as is possible:

1. a description of the breach (i.e. when and how it occurred)
2. when, where, how and by whom the breach was discovered
3. what type of personal information was involved (e.g. a person's contact details, health records, other information)
4. what systems appear to be affected (e.g. Objective, Outlook, the office's physical security system) and
5. the cause of the breach (e.g. cyber incident, human error, loss/theft of equipment or data, system fault etc).

Timely reporting is the priority therefore, a report to the Inspector should not be made later than one business day because more time is needed to gather information that addresses all of points 1 – 5 above.

The requirement to report data breaches includes:

- breaches that have already been contained (for example, if a stolen laptop has been recovered or lost hard copy files have been returned).
- breaches that occur within an agency
- breaches that occur between public sector agencies.
- breaches that occur by an external person or entity accessing data held by a public sector agency without authorisation
- breaches that may have occurred due to an accident, inadvertence, human or technical error, and
- breaches that may have occurred due to malicious intent.

Members of the public are also encouraged to report any data breaches to the Inspector in writing using the contact options available on their website.

The Inspector will then review the information provided to determine whether it is an eligible data breach under the MNDB Scheme, complete the Data Breach Report Action Plan and include all data breaches in the Internal Data Breach Register.

7.2 Step two: contain the breach

Containing the breach is prioritised by the Inspector. All necessary and reasonable steps possible must be taken immediately to contain the breach and minimise any resulting damage.[4] For example, recover the personal information, shut down the system that has been breached, suspend the activity that led to the breach, or revoke or change access codes or passwords.

If the Inspector identifies that the breach may be a cyber security incident or involve IT systems, the Inspector will consult with the Chief Information Security Officer and/or Chief Digital & Information Officer. The Inspector will delegate the function under section 59E(2)(a) of the PPIP Act to the PD's Chief Information Security Officer and Chief Digital & Information Officer so that in the event of a cyber security incident that is also a data breach, appropriate action can be taken to contain the breach.

If at this or any later step the Inspector identifies that:

- the breach may be of PD and/or TCO information, or
- the breach may be of the Inspector's information contained in the PD and/or TCO's systems,

the Inspector will liaise with the **Director, Information and Privacy – Legal Branch** to confirm application of The Cabinet Office and Premier's Department Data Breach Policy and/or the Inspector's Data Breach Policy.

If a third-party is in possession of the data and declines to return it, it may be necessary for the Inspector to seek legal or other advice on what action can be taken to recover the data. When recovering data, the Inspector will make sure that copies have not been made by a third party or, if they have, that all copies are recovered. This can include receiving written confirmation from a third-party that the copy of the data that they received in error, has been permanently deleted.

[4] s 59E(2)(a) PPIP Act.

7.3 Step three: assess and mitigate

7.3.1 Assess

To determine what other steps are needed, the Inspector will undertake an assessment of the type of data involved in the breach, whether the breach is an eligible breach under the MNDB Scheme, and the risks and potential for serious harm associated with the breach. The Inspector may direct one or more persons to carry out the assessment. However, a person who the head of the agency reasonably suspects was involved in an action or omission that led to the breach is not permitted to be an assessor. [5]

The assessment must be done with 30 days after becoming aware of the breach.[6] If the Inspector is satisfied an assessment cannot reasonably conducted within 30 days, they may approve an extension.[7] If an extension is approved, notice will be given to the Privacy Commissioner.[8] The Privacy Commissioner may ask the Inspector for further information about the progress of the assessment.[9]

To conduct this assessment:

- all relevant information will be gathered regarding the suspected breach (for example by contacting relevant stakeholders and identifying what information was or may have been compromised, investigating evidence of compromise to systems)
- the information gathered will be analysed
- the IPC's 'Data Breach Self-assessment Tool for Mandatory Notification of Data Breach'[10] will be used and
- guidelines on the assessment of data breaches under Part 6A of the PPIP Act[11] prepared by the NSW Privacy Commissioner will be considered.[12]

Following assessment, the assessor (if not the Inspector) must advise the Inspector whether the assessment found:

c. the data breach is an eligible data breach, or

d. there are reasonable grounds to believe the data breach is an eligible data breach.[13]

After receiving the assessor's advice or when the Inspector completes their assessment, the Inspector must decide whether:

a. the data breach is an eligible data breach, or

b. there are reasonable grounds to believe the data breach is an eligible data breach.[14]

A Data Breach Response Action Plan will be used for reporting on the investigation of the breach and authorising actions in response. The Inspector will be responsible for the implementation of proposed actions and recommendations.

---

[5] s 59G PPIP Act.

[6] s 59E(2)(b) PPIP Act; s 59G(4) PPIP Act.

[7] s 59K(1) PPIP Act.

[8] See s 59K (3)-(4) PPIP Act.

[9] s 59K(5) PPIP Act.

[10] https://www.ipc.nsw.gov.au/Data-breach-self-assessment-tool

[11] https://www.ipc.nsw.gov.au/guidelines-assessment-data-breaches-under-part-6a-ppip-act

[12] s 59I PPIP Act.

[13] s 59J(1) PPIP Act.

[14] s 59J(2) PPIP Act.

Some types of data are more likely to cause harm if it is compromised. For example, personal information, health information, and security classified information will be more significant than names and email addresses on a newsletter subscription list. Given the Inspector's functions release of complaint-related personal information will be treated very seriously.

A combination of data will typically create a greater potential for harm than a single piece of data (for example, an address, date of birth and bank account details, if combined, could be used for identity theft).

Factors to consider when assessing a data breach include:[15]

- who is affected by the breach?
  - have individuals and organisations been affected?
  - how many individuals and organisations have been affected?
  - do any of the individuals have personal circumstances which may put them at particular risk of harm?
- What was the cause of the breach?
  - was it part of a targeted attack?
  - was it through inadvertent oversight?
  - was it a one-off incident, has it occurred previously, or does it expose a more systemic vulnerability?
  - what steps have been taken to contain the breach?
  - has the data or personal information been recovered?
  - is the data or personal information encrypted or otherwise not readily accessible?
- What is the foreseeable harm to the affected individuals/organisations?
  - what possible use is there for the data or personal information?
  - what is the type of data? E.g. health data.
  - would the information or data be used for identity theft or lead to threats to physical safety, financial loss, or damage to reputation?
  - who is in receipt of the data?
  - what is the risk of further access, use or disclosure, including via media or online?
  - if complaint related, does it risk embarrassment or harm to a complainant and/or damage the Inspector's reputation?

7.3.2 Mitigate

During the assessment the Inspector must take all reasonable steps to mitigate the harm done by the suspected breach.[16]

The Inspector will delegate the function under section 59H of the PPIP Act to the PD's Chief Information Security Officer and Chief Digital & Information Officer so that where a cyber security incident is a data breach appropriate action can be taken to mitigate.

To mitigate the breach, the Inspector will also consider (and where relevant consult with the Chief Information Security Officer and/or Chief Digital & Information Officer) the following measures:

[15] s 59H PPIP Act.

[16] s 59F PPIP Act.

- implementation of additional security measures within Inspector's own systems and processes to limit the potential for misuse of compromised information
- limiting the dissemination of breached personal information. For example, by scanning the internet to determine whether lost or stolen information has been published and seeking its immediate removal from public sites
- engaging with relevant third parties to limit the potential for breached personal information to be misused for identity theft or other purposes, or to streamline the re-issue of compromised identity documents. For example, contacting an identity issuer or financial institution to advise caution when relying on particular identity documents for particular cohorts.

7.4 Step four: notify

If an eligible data breach has occurred, the notification process under Division 3 of the MNDB Scheme (Part 6A of the PPIP Act) is triggered.[17] There are four elements of the notification process:

1. Notify the Privacy Commissioner immediately[18] after an eligible data breach is identified using the approved form.[19]
2. Determine whether an exemption applies: If one of the six exemptions set out in Division 4 of the MNDB Scheme[20] applies in relation to an eligible data breach, the Inspector may not be required to notify affected individuals. The IPC has produced guidance to agencies on exemptions from notification.[21]
3. Notify individuals: unless an exemption applies, notify affected individuals or their authorised representatives as soon as reasonably practicable.[22]
4. Provide further information to the Privacy Commissioner in the approved form that was not given as part of the immediate notification.[23]

If a data breach is not an eligible data breach under the MNDB Scheme, the Inspector may still consider notifying individuals/organisations of the breach dependent upon the type of information that is involved, the risk of harm, repeated and/or systematic issues and the ability of the individual to take further steps to avoid or remedy harm.

Notification should be undertaken promptly to help to avoid or lessen the damage by enabling the individual/organisation to take steps to protect themselves. The MNDB Scheme requires an agency to take reasonable steps to notify affected individuals as soon as practicable.

The method of notifying affected individuals/organisations will depend in large part on the type and scale of the breach, as well as immediately practical issues such as having contact details for the affected individuals/organisations.

7.4.1 Further information about exemptions from notifying individuals

As noted above, there are six exemptions from the requirement to notify individuals.

The exemptions apply in relation to eligible data breaches:

---

[17] s 59L PPIP Act.

[18] s 59M PPIP Act.

[19] https://www.ipc.nsw.gov.au/form-data-breach-notification-privacy-commissioner

[20] The exemptions set out in Division 4 of the PPIP Act do not affect an agency's obligation to make a notification to the Privacy Commissioner.

[21] https://www.ipc.nsw.gov.au/fact-sheet-mandatory-notification-data-breach-scheme-exemptions-notification-requirements

[22] s 59N PPIP Act.

[23] s 59Q PPIP Act.

a. of multiple public sector agencies, where one of the agencies has already notified the individual, and other preconditions as to assessment and notification to the Privacy Commissioner have been met[24]

b. where the Inspector reasonably believes notification would be likely to prejudice an investigation that could lead to the prosecution of an offence, proceedings before a court or tribunal or another matter prescribed by the regulations[25]

c. where the Inspector has taken certain action to contain and mitigate so as to avoid serious harm or result in no unauthorised access to or unauthorised disclosure of the information[26]

d. where compliance with the notification requirements would be inconsistent with a secrecy provision[27]

e. where the Inspector reasonably believes notification would create a serious risk of harm to an individual's health or safety[28]

f. where the Inspector reasonably believes notification would worsen their cyber security or lead to further data breaches.[29]

In the case of the Inspector, section 111 of the *Independent Commission Against Corruption Act 1988* (ICAC Act) will be relevant in relation to the exemption under section 59V regarding secrecy provisions.

In each case, the Inspector should consider whether compliance would be inconsistent with that section and where it would be, consider whether a direction should be made pursuant to section 111(4)(c) of the ICAC Act to permit disclosure of particular information.

The Inspector recognises that notification to individuals/organisations affected by a data breach can assist in mitigating any damage for those affected. Notification demonstrates a commitment to open and transparent governance and it may be in the public interest for a direction to be made pursuant to section 111(4)(c).

7.4.2 When to notify individuals/organisations

Unless an exemption applies, individuals/organisations affected by a data breach will be notified as soon as practicable. Whilst this policy sets a target of notification within 5 days; practical factors are also recognised. Where all individuals affected by an eligible data breach cannot be notified, the Inspector will consider issuing a public notification on their website.[30]

7.4.3 How to notify individuals/organisations

Affected individuals/organisations should be notified directly – by telephone, letter, email or in person.

Indirect notification – such as information posted on the Inspector's website, a public notice in a newspaper, or a media release – should generally only occur where the contact information of affected individuals/organisations is unknown, or where direct notification is prohibitively expensive or could cause further harm (for example, by alerting a person who stole the laptop as to the value of the information contained). A record of any public notification of a data breach will be published

[24] s 59S PPIP Act.
[25] s 59T PPIP Act.
[26] s 59U PPIP Act.
[27] s 59V PPIP Act.
[28] s 59W PPIP Act.
[29] s 59X PPIP Act.
[30] s 59N(2) PPIP Act.

on the Inspector's website and recorded on the Public Data Breach Register for a period of twelve months.[31]

7.4.4 What to say in a notification to an individual/organisation

Section 590 of the PPIP Act sets out specific information that must, if reasonably practicable, be included in a notification:

1. the date the breach occurred
2. a description of the breach
3. how the breach occurred
4. the type of breach that occurred (for example, unauthorised disclosure, unauthorised access, loss of information)
5. the personal information included in the breach
6. the amount of time the personal information was disclosed for
7. actions that have been taken or are planned to secure the information, or to control and mitigate the harm
8. recommendations about the steps an individual should take in response to the breach
9. information about complaints and reviews of agency conduct
10. the name of the agencies that were subject to the breach
11. contact details for the agency subject to the breach or the nominated person to contact about the breach.

7.4.5 Other obligations including external engagement or reporting

The Inspector will also consider whether notification is required by contract or by other laws or administrative arrangements to take specific steps in response to a data breach. These may include taking specific containment or remediation steps or engaging with or notifying external stakeholders (in addition to the Privacy Commissioner), where a data breach occurs.

Depending on the circumstances of the data breach this could include:

- NSW Police Force and/or Australian Federal Police, where the IPC suspects a data breach is a result of criminal activity
- DCS, where a data breach could have an impact on the IPC's IT network or could affect the operations or data holdings held by another NSW government agency
- Cyber Security NSW, the Office of the Government Chief Information Security Officer and The Australian Cyber Security Centre, where a data breach is a result of a cyber security incident
- The Office of the Australian Information Commissioner, where a data breach may involve agencies under the Federal jurisdiction
- Any third-party organisations or agencies whose data may be affected
- Financial services providers, where a data breach includes an individual's financial information
- Professional associations, regulatory bodies or insurers, where a data breach may have an impact on these organisations, their functions and their clients
- The Australian Cyber Security Centre where a data breach involves malicious activity from a person or organisation based outside Australia.

[31] s 59P PPIP Act.

7.5 Step five: review

The Inspector will further investigate the circumstances of the breach to determine all relevant causes and consider what short or long-term measures could be taken to prevent any reoccurrence. Depending on the nature of the breach step five may be completed as part of the assessment of the first four steps and mitigation of the breach as detailed in step three above.

Preventative actions could include a:

- review of the Inspector's IT systems and remedial actions to prevent future data breaches
- security audit of both physical and technical security controls
- review of policies and procedures
- review of staff/contractor training practices
- review of contractual obligations with contracted service providers.

Any recommendations to implement the above preventative actions are to be approved by the Inspector and recorded.

8 Communication

The Inspector will be responsible for all communications issued under this Policy.

9 Record keeping

The Inspector will cause appropriate records to be maintained of how suspected breaches are managed. This includes breaches that are not notified to the Privacy Commissioner.

10 Contacts

- Inspector
  (02) 9228 3023
  oiicac_executive@oiicac.nsw.gov.au
  GPO Box 5341, Sydney NSW 2001
- The Cabinet Office | Premier's Department
  (02) 9228 5555
- Information and Privacy Commission (NSW)
  1800 472 679
  ipcinfo@ipc.nsw.gov.au
- Office of the Australian Information Commissioner
  1300 363 992
  enquiries@oaic.gov.au

11 Related documents

This policy should be read with the:

- Data Breach Response Plan
- The Cabinet Office and Premier's Department Data Breach Policy

Office of the Inspector of the Independent Commission Against Corruption

GPO Box 5341
Sydney NSW 2001

T: 02 9228 3023
W. oiicac.nsw.gov.au

NSW GOVERNMENT