Office of the
Children's Guardian

NSW GOVERNMENT

OCG Data Breach Policy

Contents

Introduction

An appropriate and effective approach to responding to data breaches can reduce the impact of a breach on individuals and the Office of the Children's Guardian (**OCG**), and may prevent future breaches.

The OCG is subject to the Mandatory Notification of Data Breach (**MNDB**) Scheme, which is established under Part 6A of the Privacy and Personal Information Protection Act 1998 (**PPIP Act**). Under the MNDB Scheme, the OCG must notify the Privacy Commissioner and affected individuals of "eligible data breaches" (discussed below). The MNDB Scheme also requires us to publish a Data Breach Policy, and maintain an internal register and public register of eligible data breaches.

This Policy provides guidance to OCG staff and contractors of the OCG on how to respond to a data breach (or suspected data breach) of OCG-held personal information, in accordance with the requirements of the PPIP Act.

This Policy outlines:

- how to identify a data breach, including an eligible data breach;
- the roles and responsibilities for reporting, managing and reviewing data breaches;
- the steps involved in dealing with a data breach and preventing future data breaches.

This Policy applies to all staff and contractors of the OCG, including temporary and casual staff, and private contractors. This Policy also applies to third party providers who hold personal information on behalf of the OCG.

What is a data breach?

A data breach occurs when personal or health information held the OCG (whether in hard copy or digital format) 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.

Personal information is "held" by the OCG if:

- The OCG is in possession or control of the information; or
- The information is contained in a State record in respect of which the OCG is responsible under the *State Records Act* 1998.

A data breach may occur:

Where	Example
Internally within the OCG	• An OCG employee views a person's records stored on an OCG database, without a legitimate purpose • An OCG employee sends a record containing an individual's personal information to a third party without authority
Between the OCG and another agency	An agency is provided access to the OCG's data as part of an inter-agency project, and an employee of the other agency uses that access for a purpose unrelated to the project
Externally outside the OCG	Personal information is accessed by a person external to the OCG during a cyberattack.

A data breach may occur due to human error, systems failure, or malicious or criminal action. Below are examples of data breaches:

Type of error	Examples
Human error	• an email or letter containing personal information is sent to the wrong recipient • a paper record or a digital device containing personal information is lost or misplaced • an unredacted record is accidentally sent to a third party (for example, a researcher or the media) instead of a copy of the record with redactions applied to the personal information • unauthorised access or disclosure of personal information because it was not disposed of in a secure manner • unauthorised access or disclosure of personal information due to a misunderstanding or lack of knowledge of whether the conduct is permitted under the Information Protection Principles set out in the PPIP Act
Systems failure	• a system error allows access to a database without authentication • inappropriate access controls on a database or document management system allow records to be visible or accessed by unauthorised individuals • a system error results in automatically generated notices containing personal information being sent to the wrong recipients
Malicious or criminal action	• theft of a paper record or digital device containing personal information • cyber incidents (for example, hacking, phishing, malware) resulting in unauthorised access to, or disclosure of, personal information

What is an eligible data breach?

The MNDB Scheme applies where an "eligible data breach" has occurred. An eligible data breach occurs when there is a data breach **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.

Under the MNDB Scheme, the definition of personal information 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**). It follows 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, including:

- name, address, phone number or date of birth
- ethnic or racial origin
- religious or philosophical beliefs
- criminal record

- photographs, images, video or audio footage
- an individual's physical or mental health, or disability.

A "reasonable person" is a hypothetical individual who is properly informed with sound judgement.

The term "serious harm" is not defined in the PPIP Act. However, guidance from the Information and Privacy Commission (**IPC**) indicates that serious harm occurs where the harm arising from the 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 irritation, annoyance or inconvenience.

The harm(s) that can arise because of a data breach will vary depending on the circumstances. For example:

- the type and level of sensitivity of personal information accessed, disclosed or lost
- the circumstances in which the data breach occurred
- the persons who were provided unauthorised access to the personal information, and the likelihood of them misusing that information.

Serious harm to an individual may include:

Type of harm	Example
Physical, psychological or emotional harm	An individual is subjected to threats to their physical safety or harassment after another person gains unauthorised access to their personal information. Note: the harm to some individuals may be exacerbated due to their personal circumstances or profession (for example, individuals impacted by family or domestic violence, police officers, judicial officers).
Financial or material harm	An individual is exposed to identity theft or fraud after their identity documents were disclosed without authorisation
Reputational harm or discrimination	An individual is exposed to discrimination or their reputation is damaged due to unauthorised disclosure of information regarding their medical history or criminal history

Roles and responsibilities

The following OCG staff have identified roles under this Policy:

Role	Responsibilities include
General Counsel / General Counsel Directorate	• Receive reports of suspected eligible data breaches, and co-ordinate the response. • General Counsel Directorate officers to undertake assessment of suspected eligible data breaches. • General Counsel to review and approve recommendations made by assessors. • General Counsel to co-ordinate notification to the

	IPC, affected individuals, and external bodies. • Maintain the internal eligible data breach register. • Review and update the Data Breach Policy as required.
Corporate Services Directorate	• Co-ordinate teams within the Directorate to assist in the response to a data breach
Manager, IT	• Establish the cause and impact of a breach involving IT systems. • Assist in containment, mitigation of harm, and implementation of preventative/remedial action. • Provide information to assist in the assessment of data breaches (Step 4, below). • Provide advice on review of security and monitoring controls related to breaches, and preventative or remedial action.
Media and Communications	• Maintain the public notification register and publish public notifications on the OCG's website. • Respond to enquiries from media and external stakeholders.
Human Resources (if appropriate)	Co-ordinate matters relating to alleged misconduct by employees and contractors connected with data breaches
OCG staff and contractors	• Immediately report a data breach or suspected data breach in accordance with this Policy. • Take reasonable steps to contain a data breach and mitigate any potential harm that may result from a data breach. • Take steps to prevent reoccurrence of a data breach.

Processes and systems to prepare for a data breach

The OCG's IT network and infrastructure is managed by the Department of Customer Services which has implemented a number of cyber security measures to mitigate the risk of data breaches. This includes:

- automated password updates so OCG staff regularly change their computer login password;
- email alerts sent to staff regarding cyber vulnerabilities and fixes;
- cyber security training to assist staff to identify possible causes of data breaches and how to detect and report suspicious online activity.

When the OCG sends personal information to external stakeholders in connection with our work, we have safeguards in place if the personal information does not reach its intended recipient. For example, data is stored on encrypted USBs, and email attachments containing sensitive information are password-protected.

Where it is necessary for personal information to be transferred to a third-party in connection with the provision of a service to us, we ensure that our contracts or memoranda of understanding or agreements with these third-party service providers include provisions:

- in relation to the management and notification of data breaches;
- impose privacy obligations to ensure that the parties comply with the PPIP Act and HRIP Act.

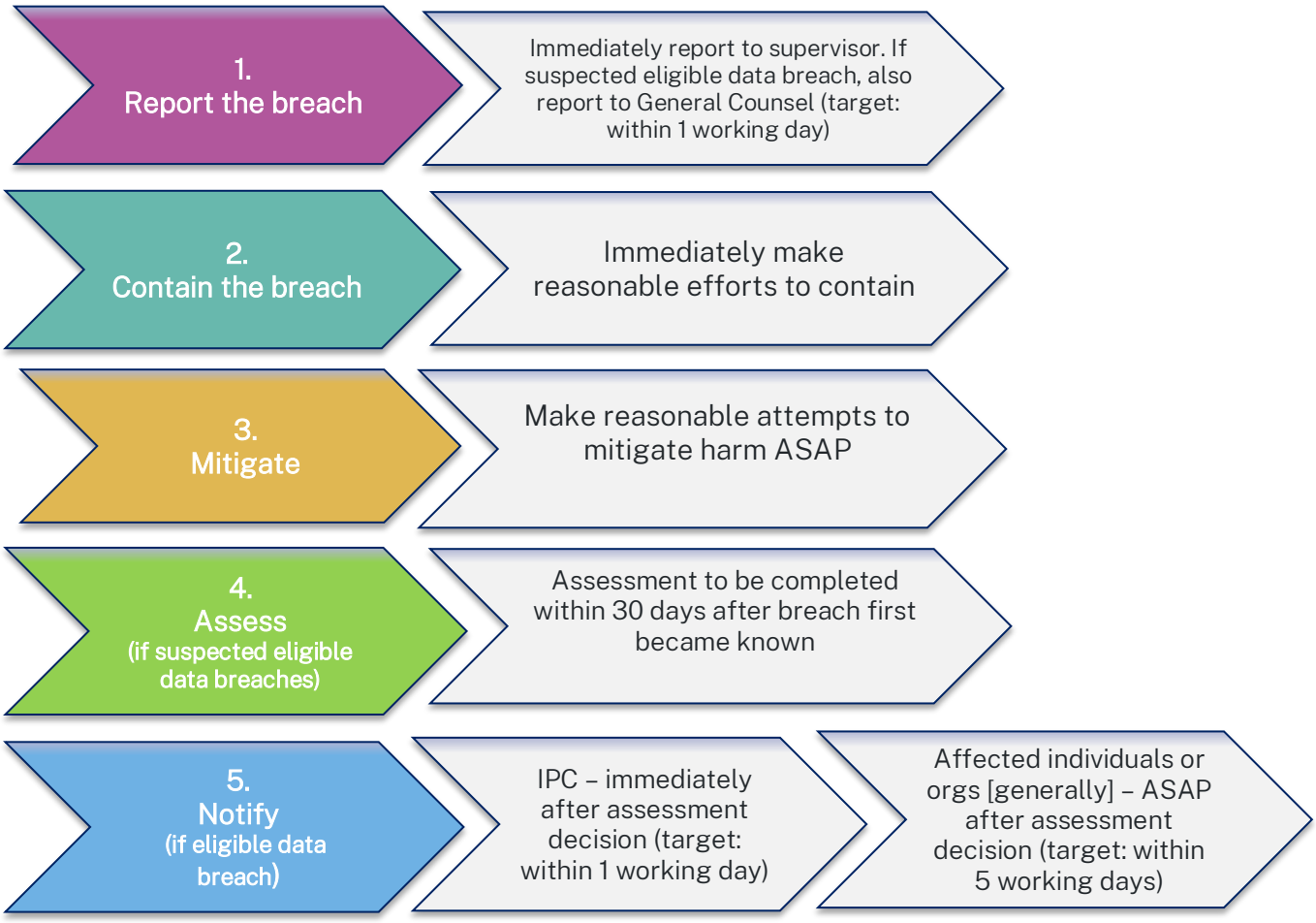
The OCG will ensure all third-party service providers who receive OCG held personal information in connection with the provision of a service to us, are aware of the MNDB Scheme and the obligations under this Policy to report any data breaches to the OCG.

Training will be provided to OCG staff on the MNDB Scheme, and how to report and respond to data breaches. The OCG will continually review the training needs of staff with respect to data breaches.

Please see the OCG's Privacy Management Plan for further information about other measures that we have implemented to prevent and manage data breaches.

Responding to a data breach

The OCG's procedure for responding to a data breach comprises the steps set out below. All steps apply to an eligible data breach (or suspected eligible data breach). Steps 1, 2, 3 and 6 apply to all data breaches, regardless of whether it is an eligible data breach (or suspected eligible data breach).



Each step is set out in detail below.

Step 1: Report the data breach

If a staff member, contractor or third-party provider (**the reporter**) becomes aware of a data breach, they must immediately notify their direct supervisor (where applicable), so that an initial assessment is made as to whether there are reasonable grounds to suspect that the breach is an eligible data breach (see: **'What is an eligible data breach?'**, above). The supervisor should document the reported data breach for record-keeping purposes.

If there are reasonable grounds to suspect that there may have been an eligible data breach, the reporter must report the matter to General Counsel by email to privacy@ocg.nsw.gov.au. This process should be completed **within one (1) working day** of the reporter becoming aware that a data breach has, or may have, occurred.

Whether there are "reasonable grounds to suspect" is an objective test and will depend on the facts and circumstances in each case. If there is any doubt as to whether an eligible data breach has occurred, or may have occurred, the matter should be reported to General Counsel for confirmation.

The information to be provided by the reporter includes:

- when, where and how the data breach was discovered
- the type of personal information involved
- the type of data breach (for example, unauthorised use, loss etc)
- the number of individuals who are or might be affected by the data breach
- the actions undertaken to contain the breach
- where the breach relates to a contracted service provider, a copy of the relevant signed contract (this will assist General Counsel to determine whether there are any other additional obligations relating to managing the breach).

This information is to be recorded by the General Counsel Directorate on the OCG's internal register for eligible data breaches (**Internal Register**). The Internal Register is to be updated with further information as the matter progresses. The General Counsel Directorate will save documents provided as part of the report on the OCG's document management system.

Members of the public are encouraged to report any data breaches to the OCG by email to privacy@ocg.nsw.gov.au, or by using the contact options available on our website: https://ocg.nsw.gov.au/contact-us

Step 2: Contain the data breach

An **immediate priority** is to contain the breach. All necessary and possible steps must be taken to contain the breach and minimise any resulting damage. To identify the appropriate strategy to contain the data breach, consider the following:

- how did the breach occur?
- is the personal information still being shared, disclosed, or lost without authorisation?
- who has access to the personal information?
- what can be done to secure the information, or stop the unauthorised access or disclosure, and reduce the risk of harm to affected individuals?

Strategies to contain a data breach include:

- recovering the affected information from a third party
- suspending the activity that led to the breach
- shutting down the system that caused the breach and addressing security weaknesses
- revoking or changing passwords or access codes.

If the containment strategy involves securing or shutting down breached systems or revoking or changing computer access codes, the Director, Corporate Services will contact the IT Manager and ensure the shutdown or changes occur as soon as possible.

If a third party receives the personal information of another person in error, the third party must be contacted by the fastest means possible (telephone or email) to inform them of the breach of privacy, and to instruct them to return or destroy the information, or to delete any electronic records without first reading, making copies or forwarding to any other party. If the third party is contacted by telephone, this must be followed by written correspondence to the third party, asking them to confirm that they have not retained any copies of the information in their possession. If the third party declines to destroy or return the information, it may be necessary to seek legal advice from the General Counsel Directorate, or other advice, on what action can be taken to recover the information.

When implementing a containment strategy, it is important not to destroy any evidence that may be valuable in identifying the cause of the breach.

Step 3: Mitigate the breach

The OCG must make all reasonable attempts to mitigate the harm done by any data breach (or suspected breach).

The harms that can arise because of a data breach will vary depending on the circumstances. For example:

- the type and level of sensitivity of personal information accessed, disclosed or lost;
- the circumstances in which the data breach occurred;
- the persons who were provided unauthorised access to the personal information, and the likelihood of them misusing that information.

Depending on the nature of the breach, the OCG will consider implementing measures to mitigate the breach such as:

- implementing additional security measures within the OCG's systems and processes

- where appropriate and reasonably practicable, contacting the affected individual(s) to inform them that a data breach has occurred, so that they can take steps to protect themselves such as changing account passwords or being alert to possible scams resulting from the breach (see: **'Communication strategy'** below)

- if the OCG becomes aware that the personal information has been published on a public site or platform, seeking the immediate removal of the information from the site or platform.

Step 4: Assessment

Where a suspected eligible data breach has been reported to General Counsel, an officer from the General Counsel Directorate (**the assessor**) will undertake an assessment of whether the reported breach is an eligible data breach under the MNDB Scheme. The PPIP Act requires this assessment to be carried out **within 30 calendar days** of the reporter (referred to in Step 1, above) becoming of the data breach. The assessment must be carried out expeditiously. This means that the 30 days should be treated as the maximum timeframe to complete the assessment.

Whilst the PPIP Act does not specify a procedure as to how the OCG must conduct an assessment, the assessment process will generally involve:

- information-gathering: collect all relevant information regarding the breach or suspected breach (for example, contacting relevant stakeholders, consulting with relevant directorates or officers within the OCG, obtaining documentary records)
- analysis: careful review and consideration of the information gathered
- decision: determine whether the data breach is an "eligible data breach" based on the analysis.

The assessment will have regard to guidelines issued by the Privacy Commissioner about the process for carrying out an assessment.

Section 59H of the PPIP Act sets out a non-exhaustive list of factors that may be considered by the assessor carrying out the assessment of whether the data breach is (or there are reasonable grounds to believe the data breach is) an eligible data breach. Factors to consider include:

Factor	Considerations
What personal information was involved in the breach?	Some types of information are more likely to cause harm if it is compromised. For example, security-protected information, or sensitive personal or health information are more significant than disclosure of personal information such as names or email addresses only. A combination of personal information will typically create a greater potential for harm than a single piece of information. For example, date of birth and bank account details, if combined, could be used for identity theft).
Who is affected by the breach?	• Individual or organisation? • How many individuals or organisations are affected? • Does the individual's personal circumstances put them at particular risk of harm?
What was the cause of the	• Human error, systems failure, or malicious or criminal act?

breach?	• Does it expose an underlying systemic vulnerability? • Was it a one-off incident or has it occurred before?
What is the foreseeable harm to affected individuals or organisations?	• What is the possible use(s) for the personal information/data? • Who is in receipt of the personal information/data? • What is the risk of further access, use or disclosure? • What harm has occurred? • What steps have been taken to contain the breach? • Has the personal information/data been recovered? • Is the personal information/data encrypted or otherwise not readily accessible?
Guidance issued by the Privacy Commissioner about eligible data breaches	IPC Guidelines on the assessment of data breaches under Part 6A of the PPIP Act

The assessor will prepare a Data Breach Report setting out matters including:

- information about the assessment process, including the assessor's analysis of the information before them, and the factors listed under section 59H of the PPIP Act
- whether the assessment found the data breach is an eligible data breach, or there are reasonable grounds to believe the data breach is an eligible data breach
- proposed actions and recommendations.

The Data Breach Report will be submitted to General Counsel for approval. The appropriate officer/directorate will be responsible for the implementation of approved actions and recommendations.

The Data Breach Report and any associated records are to be saved on the OCG's document management system.

Step 5: Notify

Where the breach is an eligible data breach

If, following the assessment process, it is decided that an eligible data breach has occurred, the notification process under the MNDB Scheme is triggered (see: Part 6A, Division 3 of the PPIP Act). The OCG **must** take the following steps as part of this process:

- Immediately notify the Privacy Commissioner of the eligible data breach, using the approved form, and
- Take reasonable steps to notify affected individuals as soon as practicable, unless one of the exemptions set out in Part 6A, Division 4 of the PPIP Act applies.

General Counsel is responsible for co-ordinating the notification process in this Policy.

Privacy Commissioner

This Policy sets a target for notification of the Privacy Commissioner **within one (1) working day** of the OCG's decision that an eligible data breach has occurred, but this timeframe is subject to practical factors. The notification to the Privacy Commissioner is to be made using the approved form on the IPC's website.

Any information that was not provided to the Privacy Commissioner as part of the immediate notification, must be provided using the approved form. This is to occur following notification of affected individuals, or (if an exemption under Part 6A, Division 4 of the PPIP Act applies) following General Counsel determining that an exemption applies.

Affected individuals

An "affected individual" is defined under section 59D of the PPIP Act as an individual:

- to whom the information subject to data breach relates; and
- who a reasonable person would conclude is likely to suffer serious harm as a result of the data breach.

Before proceeding with notifying affected individuals, a determination should be made as to whether an exemption set out in Part 6A, Division 4 of the PPIP Act applies to the eligible data breach. The exemptions are:

1) Multiple public sector agencies are involved in the same eligible data breach and one of those agencies undertakes to notify affected individuals of the breach,

2) General Counsel reasonably believes that notifying affected individuals of the eligible data breach would be likely to prejudice matters such as an ongoing investigation that could lead to the prosecution of an offence, or proceedings before a court or tribunal,

3) The agency has taken certain action to mitigate:

    - the harm done by an eligible data breach such that a reasonable person would conclude that the unauthorised access to, or disclosure of, personal information would not be likely to result in serious harm to an individual, or
    - the loss of personal information such that there is no unauthorised access to, or unauthorised disclosure of, the information,

4) Notifying affected individuals would be inconsistent with secrecy provisions,

5) General Counsel reasonably believes notification of affected individuals would create a risk of harm to an individual's health or safety,

6) General Counsel reasonably believes notification would worsen the agency's cyber security or lead to further data breaches.

If an exemption applies, the OCG may not be required to notify affected individuals for a particular matter.

If an exemption does not apply, affected individuals should be notified as soon as practicable after the OCG decides that an eligible data breach has occurred. This Policy sets a target for notification of affected individuals **within five (5) working days** of the OCG's decision that an eligible data breach has occurred, but this timeframe is subject to practical factors.

The method of notifying affected individuals will depend on the type and scale of the breach, and practical issues such as whether each affected individual can be contacted. Where the affected individual(s) can be contacted, they should be notified directly (for example, telephone, email or letter). Where all individuals affected by an eligible data breach cannot be notified (for example, because their contact details are unknown and cannot reasonably be obtained, or direct notification

is prohibitively expensive), the OCG will issue a public notification on its website and the matter will be recorded on the OCG's Public Notification Register for a period of 12 months on the OCG's website.

The OCG **must** provide the Privacy Commissioner with information about how to access the notification on the Public Notification Register as soon as practicable after the notification is published.

Section 59O of the PPIP Act sets out the information that must be included in a notification to affected individuals, if it is reasonably practicable to do so:

- The date the breach occurred
- A description of the breach
- How the breach occurred
- The type of breach that occurred (for example, unauthorised disclosure, unauthorised access, loss of information)
- The personal information that was breached
- The amount of time the personal information was disclosed for
- Actions that have been taken or are planned to ensure the information is secure, or to control or mitigate the harm done to the individual
- Recommendations about the step the individual should take in response to the breach
- Information about how to make complaints or seek review of the agency's conduct
- The name of the agencies that were the subject of the breach
- Contact details for the agency or the person nominated by the agency as the point of contact.

External bodies

The OCG will also consider whether notification to an external body is required or appropriate. For example, notification is required by a contract/memorandum of understanding/agreement, or by the circumstances of the breach.

This could include:

External body	Circumstances
NSW Police / Australian Federal Police	Where the OCG suspects a data breach is a result of criminal activity.
Department of Customer Service	Where the data breach could have an impact on the OCG's IT network, or could affect the operations or data holdings of another NSW government agency.
Cyber Security NSW / Australian Signals Directorate	Where a data breach is a result of a cyber security incident.
Any third-party organisations or agencies	Where the data of those organisations or agencies may be affected

Where notification of external stakeholders is proposed, General Counsel will consult with the Manager, IT and other directorates within the OCG as required.

Where the breach is not an eligible data breach

If a data breach is not an eligible data breach under the MNDB Scheme, the OCG may still consider notifying affected individuals of the breach on a case-by-case basis. Whilst notification demonstrates the OCG's commitment to open and transparent governance, consideration should also be given as to whether notification may be counter-productive. For example, notifying an individual about a data breach that poses very little or no risk of harm can cause them unnecessary stress or harm.

Step 6: Review and learn

The OCG will review and learn from the data breach, to consider and implement measures that could strengthen the OCG's personal information security and handling practices, and prevent similar incidents occurring in the future. The review is to be undertaken by the appropriate officer/directorate. For example, if the data breach was caused by human error, the directorate from which the breach arose should undertake the review; if the data breach was caused by a systems failure, the IT team should undertake the review.

Depending on the nature of the data breach, this step may be completed as part of the mitigation process (see: Step 3, above), or as part of the overall assessment of the OCG's response to the data breach.

Preventative actions could include a review of, and remedial action/updates in relation to:

- the OCG's IT systems;
- both physical and technical security controls;
- policies and procedures;
- employee/contractor training practices;
- contractual obligations with contracted services providers (if involved in the breach).

A data breach should be considered alongside any similar breaches that have occurred in the past, which would indicate a systemic issue with procedures or policies.

Any recommendations to implement remedial action or updates following a review are to be approved by the Director of the relevant directorate, and documented on the OCG's document management system.

OCG staff will be notified of any updates or changes to policies and procedures relating to data breaches.

Communication strategy

Prompt disclosure of a data breach to the individuals affected by a data breach can help them take steps to protect themselves and mitigate the harm or potential harm of the breach. It also demonstrates that the OCG takes privacy protection seriously.

General Counsel will be responsible for co-ordinating all communications to affected individuals, to inform them that a data breach has occurred (see: **'Step 5: Notify'** above). These communications must be dealt with sensitivity, to not exacerbate or cause further harm.

Related documents

- OCG's Privacy Management Plan

Relevant legislation

- *Privacy and Personal Information Protection Act* 1998
- *Government Information (Public Access) Act* 2009
- *Health Records and Information Privacy Act* 2002

Document information

Category	Description
Title	OCG Data Breach Policy
Directorate	General Counsel Directorate
Date of effect	28 November 2023
Next review date	28 November 2024. The review will be conducted earlier if any legislative, administrative or systemic changes affect the OCG's response to a data breach.
Document Reference	

Office of the Children's Guardian

www.ocg.nsw.gov.au

Switchboard: (02) 8219 3600

Locked Bag 5100
Strawberry Hills NSW 2012