

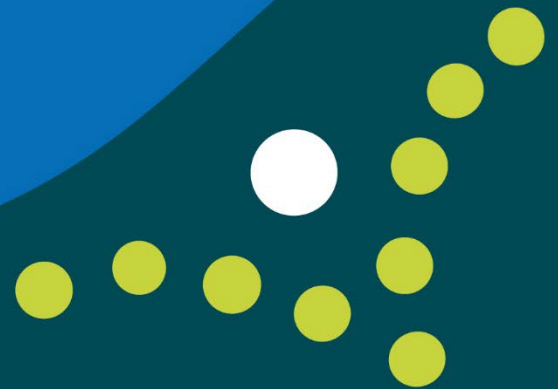


public guardian

Queensland

OPG Mandatory Data Breach Notification Policy and Response Plan

July 2025



Acknowledgement of Country

The Office of the Public Guardian acknowledges the Traditional Custodians throughout Queensland of the lands on which we leave a footprint. We acknowledge and pay our respects to their Elders, past, present and emerging.

We recognise you, the First Nations people and your continuing connection to the land, sea and waterways and acknowledge your ongoing contribution in caring for Country since time immemorial. We acknowledge your Dreamtime stories and your ancient and recent history of struggles, your strength of perseverance towards overcoming adversities and your resolve towards maintaining survival of the oldest living cultures on Earth.

Acknowledgement of living and lived experience

We acknowledge the living and lived experience of our clients, whose rights and interests we strive to promote and protect. We thank them and their support networks for engaging with us while we strive to achieve the best possible outcomes for the people we serve. We also acknowledge the living and lived experience and expertise of our staff who directly support adults with impaired decision-making ability and vulnerable children and young people in either a professional or private capacity.

Artwork acknowledgement

The OPG brand reimagines elements from within the Birrang artwork, complementing the artwork's story. The artwork Birrang (Journey) shows the journey of the OPG's clients who are adults with impaired decision-making ability and children and young people in care with OPG using the Aboriginal symbol for journeys. It features a campsite at each end of the journey representing a sense of stability when there is lots of change occurring. Various symbols in the background represent the Indigenous community's connection to Country that impacts our personal journeys and the arrows at either end of the journey symbolise overcoming adversity which often occurs for people that the OPG supports.



Birrang (Journey)
by Jordana Angus

Disclaimer

The views or opinions in this document do not necessarily reflect the views of the Department of Justice and Attorney-General or the Queensland Government. Every effort has been made to ensure this document is accurate, reliable and up to date at the time of publication, however the Office of the Public Guardian will not accept any responsibility for loss caused by reliance on this information.

Interpreter service



We are committed to providing accessible information to Queenslanders from all culturally and linguistically diverse backgrounds. If you have difficulty understanding this document, you can contact us on 1300 653 187 and we will arrange an interpreter to effectively communicate the report to you free-of-charge.

Licence

This document is licensed by the State of Queensland (Office of the Public Guardian) under a Creative Commons Attribution (CC BY) 4.0 International licence. You are free to copy, communicate and adapt this document, as long as you attribute the work to the State of Queensland (Office of the Public Guardian). To view a copy of this licence, visit creativecommons.org/licenses/by/4.0/



© The Office of the Public Guardian 2025.

Table of Contents

Purpose -----	4
Application and key definitions -----	4
Overview and Principles -----	7
Data Breach Response Plan -----	7
Responsibilities -----	13
Accountability -----	14
Additional Definitions -----	14
Authority -----	15
Consultation -----	15

Purpose

The Office of the Public Guardian (OPG) is subject to a framework of legislation, policies and standards which protect personal information. This framework includes the *Information Privacy Act 2009* (IP Act). This policy guides officers on how to respond to data breaches involving information held by OPG.

Chapter 3A of the IP Actⁱ sets out a mandatory data breach notification scheme (MDBN) scheme. As part of the MDBN scheme, OPG meets the requirement to develop and publish a data breach policy by the publication and implementation of this policyⁱⁱ.

This document defines roles and responsibilities for managing data breaches and assessing whether a privacy breach is eligible for mandatory notification under the MDBN scheme.

Application and key definitions

This policy applies to OPG employees, appointees, contractors, volunteers, and individuals undertaking work experience in OPG. This policy also applies to contracted service providers who hold personal information on behalf of OPG. This policy applies to all suspected data breaches. A reference to ‘officer’ in this policy is a reference to one or more of the foregoing.

Personal information

Personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion –

- (a) whether the information or opinion is true or not; and*
- (b) whether the information or opinion is recorded in a material form or not.ⁱⁱⁱ*

Sensitive personal information

Sensitive information, for an individual, means the following:

- (a) information or an opinion, that is also personal information, about the individual’s –*
 - (i) racial or ethnic origin; or*
 - (ii) political opinions, or*
 - (iii) membership of a political association; or*
 - (iv) religious beliefs or affiliations; or*
 - (v) philosophical beliefs; or*
 - (vi) membership of a professional or trade association; or*
 - (vii) membership of a trade union; or*
 - (viii) sexual orientation or practices; or*
 - (ix) criminal record;*
- (b) health information about the individual;*
- (c) genetic information about the individual that is not otherwise health information;*
- (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or*
- (e) biometric templates^{iv}.*

ⁱ on and from the commencement of the *Information Privacy and Other Legislation Amendment Act 2023* (IPOLA) on 1 July 2025

ⁱⁱ section 73 of the IP Act

ⁱⁱⁱ section 12 of the IP Act

^{iv} schedule 5 of the IP Act

Individual

For the purposes of the IP Act and this policy, an individual is a living person.

Affected individual

For this policy, an affected individual is an individual whose personal information or sensitive personal information is involved in a data breach or a privacy breach.

Data Breach

A data breach means either of the following in relation to information held by OPG:

- unauthorised access to, or unauthorised disclosure of, the information; or
- the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur.^v

Examples include:

Malicious or criminal attack

- cyber incidents such as ransomware, malware, hacking, phishing, or access attempts resulting in unauthorised access to, disclosure of, or theft of personal information.
- social engineering or impersonation leading to unauthorised disclosure of personal information. This includes 'insider threats' such as officers using their authentication credentials to access personal information outside of the scope of their official duties or permissions.
- theft of a physical asset such as paper record, laptop, USB stick, or mobile or smart device containing personal information.

System fault

- where a coding error allows access to a system without authentication, or results in automatically generated notices including the wrong information, or results in the information being sent to incorrect recipients.
- where systems are not maintained through the application of software updates or regular access and access privilege audits.

Human error

- where an officer does not double check the accuracy, currency, and completeness of personal information before it is used or disclosed.
- where an officer relies only on the auto-complete function in Microsoft Outlook to populate an email address without double checking the accuracy of the email address.

Eligible data breach

A data breach which involves personal information may be eligible for notification under the Mandatory Data Breach Notification (MDBN) Scheme.^{vi}

If the Corporate and Legal Practice Team (CLPT) assesses there are reasonable grounds to believe the data breach has, or will likely result in, serious harm to one or more individuals to whom the information relates, the data breach is considered an 'eligible data breach'.

^v schedule 5 of the IP Act

^{vi} Section 47 of the IP Act

Mandatory Data Breach Notification

Mandated notification to the Information Commissioner, affected individuals, or the public, about a data breach involving personal information under Chapter 3A of the IP Act.

Privacy Breach

A privacy breach is a subset of a data breach and is a breach of OPG’s obligations under the IP Act to comply with the privacy principle requirements (Queensland Privacy Principles (QPP) or a QPP Code) or the mandatory data breach notification requirements.

Queensland Privacy Principles (QPPs)

The privacy principles set out in schedule 3 of the IP Act which apply to OPG are:

- QPP1 – open and transparent management of personal information
- QPP2 – anonymity and pseudonymity
- QPP3 – collection of solicited information
- QPP4 – dealing with unsolicited information
- QPP5 – notification of the collection of personal information
- QPP6 – use or disclosure of personal information
- QPP10 – quality of personal information
- QPP11 – security of personal information
- QPP12 – access to personal information
- QPP13 – correction of personal information

QPP Code

A QPP Code is a written code of practice about information privacy that is approved by regulation.^{vii}

Serious Harm

Serious harm is harm arising from the data breach which has, or may, result in a real and substantial detrimental effect to an individual. Serious harm includes, for example:

- *serious physical, psychological, emotional, or financial harm to the individual because of the access or disclosure;*
- *serious harm to the individual’s reputation because of the access or disclosure^{viii}.*

Examples of harm include:

- identity theft
- financial loss
- threats to personal safety
- loss of business or employment opportunities
- humiliation and embarrassment
- damage to reputation or relationships
- discrimination, bullying, or other forms of disadvantage or exclusion.

^{vii} Section 40 of the IP Act

^{viii} schedule 5 of the IP Act

Data Breach Response Team (DBRT)

The Data Breach Response Team (DBRT) will comprise of any one or more of the following officers: a Deputy Public Guardian; the Director Community Visiting and Advocacy (North); the Director Community Visiting and Advocacy (South); the Director Strategy and Practice Quality; the Director Corporate Services; the Director Investigations and Guardianship (North); the Director Guardianship (South); and CLPT. These positions may delegate membership of the DBRT to another officer in their directorate.

The function of the DBRT is to review CLPT's advice and make the mandatory notifications required under the MDBN Scheme.

The DBRT will further assess the mandatory data breach notification requirements which may apply to the privacy breach and make, in consultation with relevant business areas, the required notifications.

Overview and Principles

Policy Intent

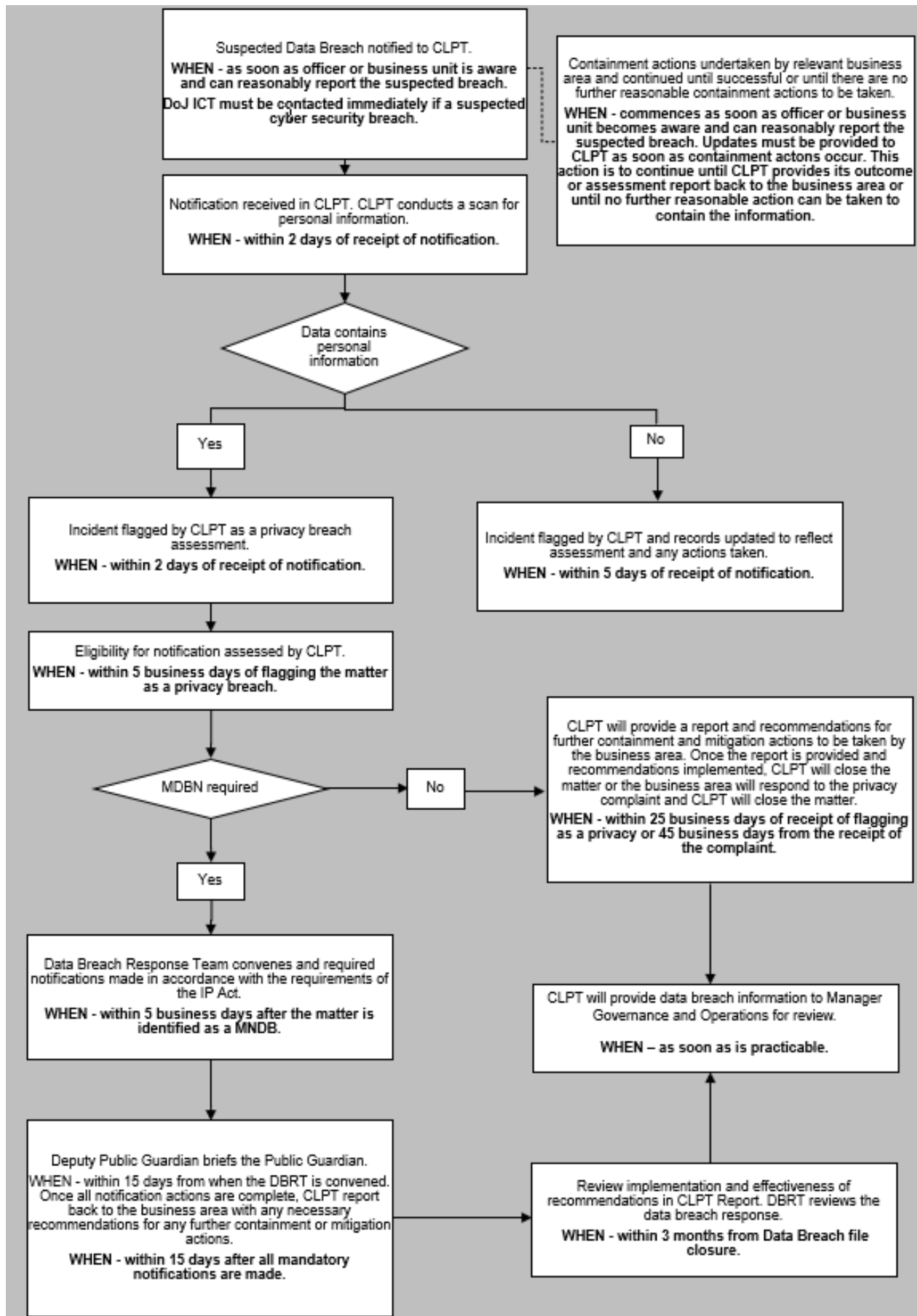
This policy reflects OPG's position on the reporting and management of data breaches. It also sets out the procedures for managing data breaches, privacy breaches and eligible privacy breaches. Eligible data breaches relate only to privacy breaches and not data breaches.

Policy Principles

- OPG values the protection of personal information held by it and respects the right of individuals to preserve the privacy of their interactions with OPG.
- OPG complies with the IP Act, including Chapter 3A of the IP Act, which creates a MNDB scheme and requires OPG to keep an internal register of data breaches eligible for notification (eligible data breaches) under the MNDB scheme.
- OPG recognises that notification to individuals and/or organisations affected by a data breach can assist in mitigating any damage for those affected individuals or organisations. Notification demonstrates a commitment to open and transparent governance.
- OPG empowers its officers to take proactive steps to manage its data lawfully and to protect the data information they manage daily. OPG does this through mandated IP Act training, mandated information security and record-keeping training and through its systems and processes for managing data breaches. The loss of IT systems because of a cyber security incident is included in the Department of Justice (DoJ) Business Continuity Plan and DoJ has included the risk of a cyber security incident into its Risk Register and established controls to mitigate the risk and impact on DoJ's systems, data, and individuals.

Data Breach Response Plan

Data Breach Response Flow Chart (next page)



These are the key steps required in responding to a suspected data breach:

- **Contain** the data breach
- Internally **report** the data breach to CLPT.
- **Classify the data breach**
- Where CLPT classify a breach as a data breach, which does not involve personal information, and the breach involves a cyber security incident, the breach will be referred to DoJ ITS for management under the relevant security playbook (see the [Cyber security incident response plan](#) for further information) and for reporting back to OPG with recommendations.
- Where data the subject of a breach contains personal information, the data breach will be managed by CLPT as a privacy breach.
- **Assess** the privacy breach - CLPT will identify associated risks, further containment actions, mitigation actions and determine whether the breach will likely result in serious harm to an individual.
- **Convene** DBRT and Notify - Where the likelihood of serious harm is assessed by CLPT, and no exemptions to mandatory notification apply under the IP Act, CLPT will notify the Deputy Public Guardian, and a Data Breach Response Team will be convened. The DBRT will meet to settle the terms and contents of the required notifications and make the required notifications to relevant individuals and organisations within 15 days from when it is stood up.
- The DBRT will nominate one of its members to brief the Public Guardian on the eligible data breach.
- Where CLPT do not identify any obligations for mandatory reporting, CLPT will manage the privacy breach as an ordinary privacy breach and report back to the business area the source of the data breach with **recommendations** for containment or mitigation, if appropriate.
- Depending on whether the data includes personal information, or a cyber security breach, ITS and/or CLPT will **review** its recommendations to the business area and the effectiveness of the recommendations made in their report back to the business area within 3 months from the delivery of the report and makes any further necessary recommendations to the business unit.

Each step is set out in further detail below.

Contain

Containing the data suspected breach is an urgent and immediate action. Where an officer suspects a data breach, the officer or their supervisor must take all possible immediate action to contain the suspected breach and minimise any resulting damage. For example, stopping the practice the cause of the breach, recovery of records lost or stolen, shutting down compromised systems, changing passwords or otherwise restricting access to the information.

Business areas must consider and report a data breach which includes information about:

- how the data breach occurred;
- whether the data is still being shared, disclosed, or is lost;
- who has or who can get access to the information;
- what can be done to secure the information, or stop the unauthorised access, disclosure or loss and reduce risk of harm to affected individuals;
- any other factor relevant to the impact on the data breach on individuals and organisations.

All records of the suspected breach, including the data the subject of it (e.g. the information sent in an email by mistake) must be preserved by the business area in accordance with the Public Records Act 2023 (PR Act). This information must be provided to CLPT when a data breach is notified.^{ix}

All records of attempts to contain the data, successful or not, must be preserved and retained in accordance with the PR Act.

Is it an email breach? If so, the business area from which suspected breach arose must take the following actions:

1. CONTAIN THE SPREAD (of information)

The priority now is to stop any further distribution of the information before it occurs. Call or email the incorrect recipient of the information AS SOON AS POSSIBLE and ask them to securely dispose of the information. The longer we wait, the harder it will be to contain the electronic transmission of information.

Do not delete the email sent to the incorrect recipient yourself. Preserve a copy for sending to CLPT.

2. Email Template

Here is a template email you can use to send to the incorrect recipient.

Good Morning/Afternoon,

You received an email from <<email address>> at <<time>> on <<date>> which was sent in error. Could the following steps please be taken and a return email sent to confirm the actions have been taken?

1. *Select the email that was sent in error*
2. *Delete to send it to your 'Deleted Items' of 'Trash' folder*
3. *Open the folder and select the email that was sent in error*
4. *Select delete*
5. *A dialog box opens and warns that the message will be permanently deleted*
6. *Select Yes*
7. *Send a reply email indicating that the above steps have been taken*
8. *If any further copies of the email exist, please advise and delete in the same manner.*
9. *Confirm you have not forwarded or printed the information sent in error.*

We apologise for any inconvenience this may have caused and thank you for taking the time to securely dispose of the information.

Kind Regards,

3. REPORT TO YOUR DIRECT SUPERVISOR

In all instances, alert your direct supervisor that you have accidentally sent an email to the wrong person and/or attached the wrong document.

4. NOTIFY CLPT OF THE BREACH AND SUBSEQUENT ACTIONS TAKEN

^{ix} Appropriate security requirements must be considered when providing this information to CLPT, and/or ITS.

Until a final assessment report is delivered by CLPT or ITS, depending on the content of the data, the business area is to continue taking all reasonable steps to contain the data by ensuring as soon as possible its destruction or return. Business areas must keep CLPT updated as containment actions occur, and whether the containment action has been successful. CLPT will update ITS if required.

If containment action is successful, the business area must provide evidence of the successful containment action. For example, a copy of the email from the unintended recipient confirming deletion from their email inbox and deleted items folders; a scanned copy of returned documents posted to the incorrect address, correspondence from the unintended recipient certifying destruction of the data.

The business area reporting the data breach must also immediately notify CLPT whether the person or entity in unauthorised possession of the information is declining to return or delete and confirm deletion of it. For example, when the unintended recipient refuses to return the information and advises they will contact the subject of the data breach and/or the media.

Internally report and refer

When a suspected data breach occurs, the officer who suspects it, or their supervisor, must notify CLPT immediately or as soon as possible after the officer becomes aware of it. An officer may become aware of a suspected data breach through a privacy complaint, or a conduct complaint made to the business area. Often, it is the unintended recipient who will make the officer aware of the suspected data breach.

Internal reporting can be a self-report directly to CLPT, or by the officer's supervisor. Internal notification may also occur at the same time the business area is undertaking the steps in STEP 1.

On becoming aware of a suspected data breach, officers must not wait to confirm whether a data breach has occurred, or to complete containment actions before reporting it to CLPT. An assessment of whether a data breach has occurred is made by CLPT and/or ITS as appropriate (for potential cyber security breach) and not the business area or the reporting officer.

Data breaches are notified immediately to CLPT in writing via email to clpt@publicguardian.qld.gov.au. A request for a meeting with CLPT may also be made at the same time.

When a complaint is received by a business unit from an individual about unauthorised access to, or disclosure of personal information, the complaint must be referred to CLPT as soon as possible after the complaint is received.

Within two business days of a suspected data breach notification, CLPT will categorise whether the information contains personal information.

For matters referred to ITS, they will follow the DoJ Mandatory Data Breach Notification Policy and Response Plan.

Where conduct or disciplinary issues arise from an assessment of a data breach, ITS or OPG will, as soon as possible after the issues are identified, refer the matter to the Ethical Standards Unit, DoJ.

Triage and assess

Where it is identified personal information is involved in a data breach, CLPT will triage the privacy breach and assess the likelihood of serious harm to the individual or individuals. If further containment action is identified as required, CLPT will also assist the business area in taking those actions.

At the same time, and within 5 business days from classifying the breach as a privacy breach, CLPT will assess the breach for eligibility to notify the Information Commissioner and relevant organisations or individuals and will consider factors including:

- *Who is affected by the breach?* CLPT’s assessment will include reviewing whether individuals and organisations have been affected by the breach, how many individuals or organisations are affected, and whether any of the individuals have personal circumstances which may put them at particular risk of harm.

For example, if the contact information of a person protected by a domestic and family violence order is disclosed to the alleged perpetrator of the violence, or the alleged perpetrator is otherwise given access to it, this will raise consideration of whether this disclosure has or is likely to amount to serious harm to the person protected by the order.

- *What was the cause of the breach?* CLPT’s assessment will include reviewing whether the breach occurred as a targeted attack or through inadvertent oversight (human error).

CLPT may consider whether: it was a one-off incident; it occurred before; it exposes a systemic gap or vulnerability; the steps taken to contain the breach; whether the data has been recovered or recoverable; if the data is encrypted or otherwise not readily accessible (for example, an eDocs reference to a document is sent but the recipient has no access to the information from eDocs).

- *What is the foreseeable harm to the affected individuals/organisations?* CLPT’s assessment will include reviewing what possible use or misuse there is for the information. This will include considering the type of personal information the subject of the breach, if it could be used for identity theft, or lead to threats to physical safety, financial loss, or damage to reputation. CLPT will also consider who has, and who can, access the information and what the risk is of further access, use or disclosure, including online or to the media and whether the incident risks embarrassment or harm to an individual and or damage the reputation of OPG.
- CLPT will also consider whether there are additional notification requirements to relevant law enforcement or cyber security bodies or regulatory bodies like the Office of the Australian Information Commissioner and advise the DBRT.

Stand up DBRT, brief, and notify

Where the likelihood of serious harm is identified by CLPT, and CLPT determine there is no applicable exemption to mandatory notification, the MDBN Scheme is triggered.

CLPT will make the Deputy Public Guardian aware of the eligible privacy breach and the Deputy Public Guardian will stand up the DBRT. CLPT will brief the DBRT on their assessment and recommended actions and notifications.

The DBRT will meet within five days of the date it is stood up to settle the mandatory notification requirements and notify relevant organisations and individuals. The DBRT will confirm whether there are any additional notification requirements to other regulatory entities such as the Office of the Australian Security Commissioner, the Office of the Australian Information Commissioner, Queensland or Australian cyber security agencies, or law enforcement bodies.

Notification will occur no later than as stipulated by the IP Act, being 30 days from OPG first becoming aware of the suspected breach.

Within 15 days from when the DBRT first convenes, the Deputy Public Guardian briefs the Public Guardian. Once all notifications are completed, CLPT will report back to the relevant business area with any necessary recommendations for any further containment or mitigation actions.

More information about mandatory data breach notifications is available [here](#).

Before there is any online (public) notification given under the MDBN scheme, the proposed notice must be cleared through the Deputy Public Guardian before publication.^x

Reporting and recommendations

If the breach is not an eligible data breach but involves personal information, it will be managed as an ordinary privacy breach by CLPT. CLPT will conduct an assessment and deliver a report back to the business area from which the breach notification is received, including giving recommendations, where necessary, for containment of the information, and for mitigation strategies to lessen the risk of repeat breaches. When matter is finalised, CLPT will provide data breach information to the Manager Governance and Operations for review.

Where CLPT identifies any conduct or disciplinary issues from its assessment, it will, as soon as possible after the issues are identified, refer these to the Deputy Public Guardian for consideration of referral to the Ethical Standards Unit, DoJ for an additional assessment.

Review

Within 3 months from delivering its report and recommendations to the business area, CLPT will review the implementation of the recommendations, assess their effectiveness since implementation, and make any further recommendations, as required.

Within 3 months from the completion of a mandatory notification process, the DBRT must review the data breach response and report on any opportunities for improvement and provide a closing off memo to the Deputy Public Guardian, Public Guardian and Manager Governance and Operations.

Responsibilities

All officers

- Responsible for reporting data breaches as soon as, or as soon as practical after they become aware of the breach. This also accords with public servants' obligations to report wrongdoing, regardless of whether it was intentional, under the Code of Conduct for the Queensland Public Service.
- Responsible for preserving records related to a data breach in accordance with the PR Act.
- Responsible for providing as much information or assistance as necessary to CLPT for the assessment of a data breach or privacy breach.

Team Leaders and Managers

- Responsible for ensuring their officers are aware of this policy and must ensure officers meet the OPG mandatory information privacy and information security training requirements.

^x If each 'individual' or 'affected individual' can't be notified, OPG must publish the required information on an accessible website for a period of at least 12 months. OPG is not required to include information in its notice if it would prejudice its functions. OPG must advise the Information Commissioner how to access the notice and the Information Commissioner is required to publish the notice on the Commissioner's website for at least 12 months.

- Responsible for ensuring the timely reporting of data breaches and for establishing local systems and processes which support the timely reporting of data breaches.

Data Breach Response Team (DBRT)

- Responsible for convening, settling the content and final terms of a notification and notifying relevant organisations and individuals within the timeframes stipulated by the IP Act.
- Responsible for reviewing the data breach response with a view to improving responses.
- Responsible for briefing the Deputy Public Guardian.
- Responsible for liaising with relevant entities and bodies, including law enforcement and regulatory bodies, throughout the data breach response and action process.

Corporate and Legal Practice Team (CLPT)

- Responsible for identifying whether a data breach involves personal information.
- Responsible for conducting privacy breach assessments for data which contains personal information.
- Responsible for advising whether mandatory data breach notification obligations arise and what they are.
- Responsible for advising the Deputy Public Guardian on whether the DBRT should convene and to provide policy guidance on mandatory notification.
- In all instances where a DBRT is convened, the CLPT will form part of the DBRT.

Deputy Public Guardian

- Responsible for the final form and content and publication of any mandatory notifications.
- Responsible for preparing the Public Guardian and DoJ and the Attorney-General for any media impact arising from a data breach.

Accountability

CLPT are accountable for ensuring the management and maintenance of this policy, including ensuring its continued appropriateness to the business, compliance with legislation and external requirements, and periodic review.

Team Leaders, Managers and Directors are responsible for monitoring, reporting and assisting in the managing data breaches relevant to their functional responsibility in OPG under the terms of this policy.

Additional Definitions

Information Privacy Act 2009 – The *Information Privacy Act 2009* (IP Act) in force on and from the commencement of the *Information Privacy and Other Legislation Amendment Act 2023* (IPOLA).

Information Privacy and Other Legislation Amendment Act 2023 – IPOLA, as consolidated into the IP Act on and from the commencement of IPOLA.

Personal Information – Defined in section 12 of the IP Act as information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion; whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not. This is a broader range of information than Personally Identifying Information (PII).

Personally Identifying Information (PII) – Information which can directly identify a person such as a name, employee number, or email address. This is a subset of the broader ‘personal information’ as defined by the IP Act.

Notifier – the person or officer who notifies CLPT about a data breach.

Office of the Information Commissioner – OIC – Queensland’s oversight and regulatory body for the *Right to Information Act 2009 and the Information Privacy Act 2009*.

Office of the Australian Information Commissioner – Commonwealth oversight and regulatory body for the *Privacy Act 1998 (Cth)*.

Officer – any person or entity referred to under ‘Application’ in this policy.

Business area – the functional business area from which a data breach arose.

Data – information.

Authority

- *Information Privacy Act 2009 (incorporating amendments made by the Information Privacy and Other Legislation Amendment Act 2023)*
- *Public Records Act 2023*
- *Public Sector Ethics Act 1994*

Consultation

This policy was developed in consultation with the OPG Corporate and Legal Practice Team.



public guardian

Queensland

