Data Breach Policy

Date policy was adopted:	28 February 2024
Resolution number:	073/24
Next Policy review date:	February 2025
Reference number:	52.5.4
Strategic Pillar	Executive Services
Responsible Branch	Governance and Legal

PURPOSE

The purpose of this policy is to guide QPRC employees in responding to a breach of QPRC-held data or information.

This policy sets out the requirements for managing a Data Breach, including the considerations around notifying persons whose privacy may be affected by the breach. It:

- Provides examples of situations considered to constitute a Data Breach;
- The steps to respond to a Data Breach; and
- Outlines the considerations around notifying persons whose privacy may have been affected by the incident.

Effective breach management assists QPRC in avoiding or reducing possible harm to both the affected individuals/organisations and QPRC. It also allows lessons to be learned that may prevent future breaches.

SCOPE

This policy applies to all QPRC employees and third party contractors.

DEFINITIONS

Term	Meaning
Data Breach	For the purposes of this policy, a data breach occurs when there is a failure that has caused unauthorised access to, or disclosure of, Confidential Information held by QPRC in both electronic and paper form.
Confidential Information	Information and data (including metadata) including Personal Information, Health Information, information protected under legal professional privilege, information covered by secrecy provisions under any legislation, commercial-in-confidence provisions, floor plans of significant buildings, and information related to QPRC's ICT and cybersecurity systems.
Data Breach Review Team	The core Data Breach Review Team comprises: • Manager Digital • Coordinator Governance and Legal (or delegate) • Risk and Internal Audit Coordinator (or delegate) • Director Corporate Services • General Manager Depending on the nature and circumstances of the breach, other employees may be called on to form part of the data breach review team.
QPRC Employee	Includes full time, part time, casual, temporary, and fixed term employees, agency staff and contractors. For the purposes of this policy, employees also include volunteers, trainees and students on work placements.

Health Information	A specific type of Personal Information which may include information about a person's physical or mental health or their disability. This includes, for example, medical certificates, information about medical appointments or test results.
Personal Information	Information or an opinion (including information or an opinion forming part of a database and whether or not in recorded form) about an individual whose identity is apparent or can be reasonably ascertained from the information or opinion. This includes, for example, their name, address, email address, phone number, date of birth or photographs.
Unauthorised Access	Examples include: • An employee browsing customer records without a legitimate purpose • A computer network/system being compromised by an external attacker, resulting in information being accessed without prior approval.

POLICY STATEMENT

QPRC will form a Data Breach Review Team, whose role it is to investigate, respond and report internally on any known or notified Data Breach involving confidential information.

There are four key steps required in responding to a reported Data Breach. These are:

1. Contain the breach
2. Evaluate the associated risks
3. Consider notifying affected individuals
4. Prevent a repeat.

The first three steps may be undertaken concurrently.

Step 1: Contain the breach

All necessary steps possible must be taken to contain the breach and minimise any resulting damage. For example, recover or request deletion of the information, shut down the system that has been breached, suspend the activity that led to the breach, evoke or change access codes or passwords.

If a third party is in possession of the personal information and declines to return it, it may be necessary for QPRC to seek legal or other advice on what action can be taken to recover the information. When recovering the information, QPRC will endeavour to ensure that copies have not been made by a third party or, if they have, recover all copies with the assistance of relevant State and Federal Agencies.

Step 2: Evaluate the associated risks

To determine what other steps are needed, an assessment of the type of information involved in the breach and the risk associated with the breach will be undertaken. Some types of information are more likely to cause harm if compromised. For example, financial account information, health information or other sensitive information will be more significant than names and email addresses on a newsletter subscription list.

Given QPRC's regulatory responsibilities, release of personal information will be treated very seriously. A combination of information 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 include:

- **Who is affected by the Data Breach?** QPRC will review whether individuals and organisations have been affected by the breach, how many individuals and organisations have been affected and whether any of the individuals have personal circumstances which may put them at particular risk of harm.

- **What was the cause of the Data Breach?** QPRC's assessment will include reviewing whether the breach occurred as part of a targeted attack or through human error or an 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 Information been recovered? Is the Information encrypted or otherwise not readily accessible?

- **What is the foreseeable harm to the affected individuals/organisations?** QPRC's assessment will include reviewing the possible malicious use of the affected information. This involves considering the type of information (such as Health Information, Personal Information subject to special restrictions under s.19(1) of the Privacy and Personal Information Protection Act 1998 which could be used for identity theft, or lead to threats to physical safety, financial loss, or damage to reputation. Who is in receipt of the information? What is the risk of further access, use or disclosure, including via media or online? If case-related, does it risk embarrassment or harm to a client and/or damage to QPRC's reputation?

Step 3: Consider notifying affected individuals/organisations

QPRC recognises that notification to individuals/organisations affected by a Data Breach can assist in mitigating any damage for those affected individuals/organisations.

Notification demonstrates a commitment to open and transparent governance, consistent with QPRC's values and approach.

QPRC will also have regard to the impact upon individuals in recognition of the need to balance the harm and distress caused through notification against the potential harm that may result from the breach. These are occasions where notification can be counterproductive. For example, notifying individuals about a privacy breach which is unlikely to result in an adverse outcome for the individual, may cause unnecessary anxiety and de-sensitise individuals to a significant privacy breach.

Factors QPRC will consider when deciding whether notification is appropriate include:

- Are there any applicable legislative provisions or contractual obligations that require QPRC to notify affected individuals?
- What type of information is involved?

- Who potentially had access, and how widespread was the access?
- What is the risk of harm to the individual/organisation?
- Is this a repeated and/or systemic issue?
- What risks are presented by the mode of the breach e.g. Is it encrypted information or contained in a less secure platform e.g. email?
- Does the breach relate to regulatory functions and include case-related material flowing from the exercise of our regulatory functions?
- What steps has QPRC taken to date to avoid or remedy any actual or potential harm?
- What is the ability of the individual/organisation to take further steps to avoid or remedy harm?
- Even if QPRC would not be able to take steps to rectify the situation, is the information that has been comprised confidential, or likely to cause humiliation or embarrassment for the individual/organisation?

In situations when notification is required, it should be done promptly to help avoid or lessen any potential damage by enabling the individual/organisation to take steps to protect themselves.

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

Considerations include the following:

When to notify

In general, individuals/organisations affected by the breach should be notified as soon as practicable. Circumstances where it may be appropriate to delay notification include where notification would compromise an investigation into the cause of the breach or publicly reveal a system vulnerability.

How to notify

Affected individuals/organisations should be notified directly – by telephone, letter, email or in person. Indirect notification – such as information posted on QPRC's website, a public notice in a newspaper, or a media release – should generally only occur where the contact information of affected individuals/organisations are unknown, or where direct notification is prohibitively expensive or could cause further harm.

What to say

The notification advice will be tailored to the circumstances of the particular breach.

Content of a notification could include:

- Information about the breach, including when it happened
- A description of what confidential or personal information has been disclosed
- What QPRC is doing to control or reduce the harm
- What steps the person/organisation can take to further protect themselves, and what QPRC will do to assist people with those steps
- Contact details for questions or requests for information
- The right to lodge a privacy complaint with the NSW Privacy Commissioner.

Step 4: Prevent a repeat

QPRC 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.

Preventative actions could include a:

- 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.

Notifying the NSW Privacy Commissioner

QPRC will notify the NSW Privacy Commissioner of a Data Breach where personal information has been disclosed, and there are risks to the privacy of individuals.

In doing so, QPRC will ensure that relevant evidence is contained securely for access by the Privacy Commissioner should regulatory action be considered appropriate. Such notification will:

- Demonstrate to the affected individuals and broader public that QPRC views the protection of personal information as an important and serious matter and may therefore maintain public confidence in QPRC; and

- Facilitate full, timely and effective handling of any complaints made to the Privacy Commissioner in regard to the breach and thus assist those whose privacy has been breached.

Notification should contain similar content to that provided to the individuals/organisations. The personal information about the affected individuals should not be provided. It may be appropriate to include:

- A description of the breach
- The type of personal information involved in the breach
- What response QPRC has made to the breach
- What assistance has been offered to affected individuals
- The name and contact details of the appropriate contact person
- Whether the breach has been notified to other external entities.

Internal notifications

The following roles will be notified of any data breach:

- Coordinator Governance and Legal
- Director Corporate Services
- Risk and Internal Audit Coordinator
- Manager Digital
- General Manager
- Manager Customer and Communication
- Data owner (Manager of the relevant business unit)

Data breach documentation

Documentation relating to data breaches will be stored in the Council records system.

Responsibilities

All employees must:

- Immediately report any actual or suspected Data Breaches to the Manager Digital and/or Coordinator Governance and Legal and/or Director Corporate Services

The Director Corporate Services will:

- Immediately notify the Data Breach Review Team and assemble the Team as soon as possible.
- Undertake relevant internal notifications as required by this policy.

The Data Breach Review Team will:

- Assemble promptly to review and respond to a data breach
- Follow this policy when responding to a data breach
- Consult with internal and external stakeholders as required
- Prepare a data breach review report for each separate Data Breach incident.

The Manager Digital will:

- Take immediate and any longer-term steps to contain and respond to security threats to QPRC's ICT systems and infrastructure

The Coordinator Governance and Legal will:

- Undertake notifications as required to affected individuals/organisations and the NSW Privacy Commissioner
- Notify QPRC's insurers as required.

LEGISLATIVE OBLIGATIONS AND/OR RELEVANT STANDARDS

Laws and Standards
• Privacy and Personal Information Protection Act 1998 • Health Records and Information Privacy Act 2002
Policies and Procedures
• IPC Data Breach Guidance for NSW Agencies (September 2020) • Information and Privacy Commission Data Breach Policy (October 2023) • QPRC Data Breach Review Report • QPRC Data Breach Notification Template Letter • Sensitive and Security Classified Information Scheme • IT Security Policy

REVIEW

This policy will be reviewed every four years or earlier as necessary if:

a) legislation requires it, or
b) Council's functions, structure or activities change