Privacy Incident Response Plan

QUEENSTOWN LAKES DISTRICT COUNCIL

CONTENTS

1 INTRODUCTION

This privacy incident response plan ('response plan') sets out procedures and clear lines of authority for Queenstown Lakes District Council (QLDC) staff in the event that QLDC experiences a privacy incident (or suspects that a breach or incident has occurred).

A privacy incident occurs when personal information is accessed or disclosed without authorisation or is lost.

Under the Privacy Act 2020, QLDC must notify affected individuals and the Office of the Privacy Commissioner | Te Mana Mātāpono Matatapu ('the Commission') when an incident or breach (referred to hereafter as just 'breach') is likely to result in serious harm to an individual (or individuals) whose personal information[1] is involved.

For good privacy practice purposes, this response plan covers any instances of unauthorised use, modification, interference with or loss of personal information held by QLDC. Breaches can be caused or exacerbated by a variety of factors, affect different types of personal information and give rise to a range of actual or potential harms to individuals and entities.

This response plan is intended to enable QLDC to contain, assess and respond to breaches quickly, to help mitigate potential harm to affected individuals and to comply with the requirements of the Privacy Act and the Commission. Our actions in the first 24 hours after discovering a breach are crucial to the success of our response.

This plan confirms officers delegated with powers, duties and responsibilities under the Privacy Act and follows a framework based on guidance[2] from the New Zealand Government | Te Kāwanatanga o Aotearoa.

2 RESPONDING TO A PRIVACY BREACH

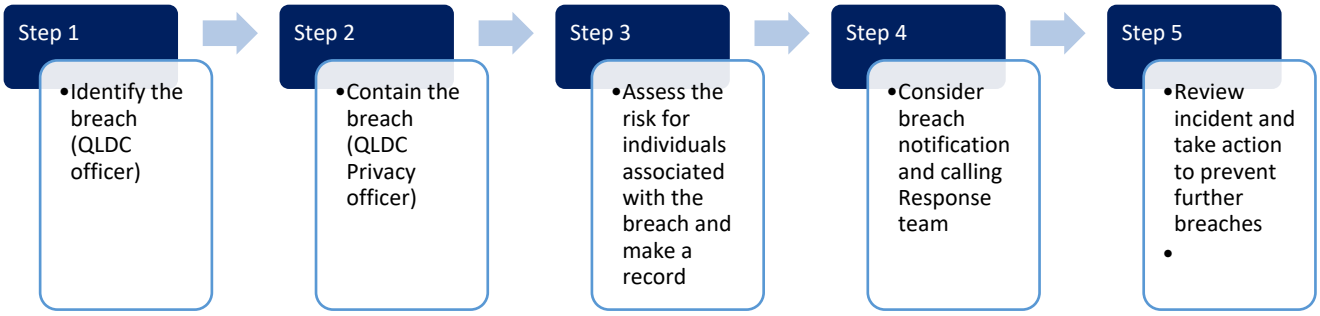
There is no single method of responding to a privacy breach. Breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action. Depending on the nature of the event, the Privacy Officer or convened response team may need to include additional staff or external experts, for example an IT specialist/data forensics expert or a People & Capability Advisor.

When responding to a breach officers should ideally undertake steps 1, 2 and 3 either simultaneously or in quick succession. At all times, officers should consider what remedial action can be taken to reduce any potential harm to individuals.

Officers should refer to the checklist below and to the Commission's guidance on responding to privacy breaches[3].

Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, it may be appropriate to take additional steps that are specific to the nature of the breach.

[1] https://www.privacy.org.nz/tools/knowledge-base/view/199?t=1318464_1480434
[2] https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/privacy-incidents-and-breaches/privacy-incident-response-plan/
[3] https://privacy.org.nz/responsibilities/privacy-breaches/responding-to-privacy-breaches/



2.1 PRIVACY BREACH RESPONSE TEAM (THE "RESPONSE TEAM")

Where an investigating Privacy Officer deems necessary, they may convene a Response team to assist in responding to an actual or suspected privacy breach. Membership of the Response team vary for every breach but will always include a minimum of one delegated privacy officer. The remaining membership will be cross-organisational and based on the type or severity of the incident. For example, a breach involving the sharing of personal information about children attending swim school would require support and input from legal, knowledge management, and communications, as well as privacy officers and sport and recreation staff.

More information about Response teams can be found in Step 4 of this plan.

3 STEP 1: IDENTIFY THE BREACH

A suspected or confirmed breach may be discovered by a QLDC staff member or contractor or QLDC may be otherwise alerted (for example, by a member of the public or the media).

If you become aware of, or are notified of a breach or suspected breach, immediately notify your direct line manager. A breach suspected by a member of the Executive Leadership team (ELT) may be reported directly to a delegated Privacy Officer. If in doubt about whether to notify, always act with caution and favour notifying your line manager and/or a Privacy Officer to ensure incidents can be responded to in a timely and appropriate manner and opportunities for learning and continuous improvement identified.

Record and advise your manager of the following:

> the time and date the suspected breach was discovered,

> the type of personal information involved,

> the cause and extent of the breach,

> mechanisms / channels for notifying the person(s) affected; and

> the context of the affected information and the breach.

4 STEP 2: CONTAIN THE BREACH AND NOTIFY A QLDC PRIVACY OFFICER

With your manager you should seek to understand, assess and contain the breach. Once a Privacy Officer is made aware of the breach or suspected breach, the Privacy Officer should seek all facts to enable an initial assessment of whether a breach has or may have occurred and the seriousness of the breach or suspected breach. This should be done within the first hour of being made aware.

The Privacy Officer should coordinate any immediate action required to contain the breach. Depending on the breach, this may include contacting incorrect recipients requesting them to delete a specific email they have received in error or requesting information be removed from a website.

The officer that identified the breach or suspected breach, or their manager, should notify the Privacy Officer about the breach, ideally by phone in the first instance, and then a follow-up email as soon as reasonably practicable after coordinating any immediate action. Notification must occur however within the same working day as being made aware of the breach and coordinating immediate action. Notification to a Privacy Officer should include the provision of the following information:

- the information provided by the QLDC officer in identifying the privacy breach (see Step 1),
- a description of the breach or suspected breach,
- the action taken by the manager or officer to address the breach or suspected breach,
- the outcome of that action,
- a view as to the seriousness of the breach, and
- a view as to whether any further action is required.

4.1 WHO ARE QLDC'S PRIVACY OFFICERS?

There are four delegated positions that hold the role of privacy officer at QLDC. These are as follows

- Chief Information Officer
- Director People & Capability
- General Counsel
- Stakeholder & Democracy Services Manager

5 STEP 3: ASSESS THE RISKS FOR INDIVIDUALS ASSOCIATED WITH THE BREACH AND MAKE A RECORD

5.1 ASSESSMENT BY A PRIVACY OFFICER

It is the Privacy Officer's role to determine whether the breach constitutes a Notifiable Breach[4]. The Privacy Officer should initially assess the breach, which may involve asking for further information or documentation from the manager and /or officer who identified and reported the breach.

Collection of the following information about the breach should form part of that assessment by the Privacy Officer:

- the date, time, duration, and location of the breach
- the type of personal information involved in the breach
- how the breach was discovered and by whom
- the cause and extent of the breach

[4] See 'When to notify' here: https://privacy.org.nz/responsibilities/privacy-breaches/responding-to-privacy-breaches/

- a list of the affected individuals, or possible affected individuals
- the risk of serious harm to the affected individuals
- the risk of other harms.

Following that assessment, the Privacy officer must decide whether any further action is required to contain the breach.

5.2 RECORD KEEPING

The Privacy Officer co-ordinates the record keeping for each privacy breach in the TechnologyOne Request Management System and documents are stored in each request.

Information about every breach will be recorded in the Request Management System request, regardless of whether the Response team is convened or the breach amounts to a Notifiable Privacy Breach. The request must include the reasons why the Privacy Officer did or did not convene the response team or classify the matter as a Notifiable Privacy Breach, with links to the relevant decision documents.

5.3 INFORMING THE EXECUTIVE LEADERSHIP TEAM AND ELECTED MEMBERS

The responding Privacy Officer is required to inform the Commissioner in the event the matter is deemed to be a notifiable event and/or triggers the formation of the Response team. If in doubt, the Privacy Officer will err on the side of caution and notify.

The Privacy Officer must inform the QLDC Executive Leadership Team as soon as possible after being made aware of a suspected or actual privacy breach and must provide ongoing updates on key developments. Those updates may be daily or weekly depending on the nature and severity of the breach, and how quickly any remedial action can be taken and resolved. The frequency of reporting will be ascertained on a case-to-case basis.

Elected members must be informed on every occasion of an actual or suspected privacy breach that is notifiable on the grounds of potential serious harm.

6 STEP 4: CONSIDER BREACH NOTIFICATION AND CALLING A PRIVACY BREACH RESPONSE TEAM

6.1 PRIVACY OFFICER TO USE DISCRETION IN DECIDING WHETHER TO ESCALATE TO THE RESPONSE TEAM

On each occasion of a privacy breach, the Privacy Officer must consider whether to convene the Privacy Breach Response Team.

Some breaches may be comparatively minor, and able to be dealt with easily without action from the response team. For example, an officer may, as a result of human error, send an email containing personal information to the wrong recipient. Depending on the sensitivity of the contents of the email, if the email can be successfully recalled (only relates to internal emails), or if the officer can contact the recipient and obtain an assurance that the recipient has deleted the email, it may be that there is no benefit in escalating the issue to the response team.

The Privacy Officer should use their discretion in determining whether a breach or suspected breach requires escalation to the response team. The decision to escalate to the response team should be made immediately following the Privacy Officer's assessment about the privacy breach after discussions with the relevant manager and/or officer and the collation of relevant material.

In making that decision the Privacy Officer should consider the following questions:

> Are multiple individuals affected by the breach or suspected breach?

> Is there (or may there be) a real risk of serious harm to any of the affected individual(s)?

> Does the breach or suspected breach indicate a systemic problem in QLDC processes or procedures?

> Could there be media or stakeholder attention as a result of the breach or suspected breach?

Once the Privacy Officer decides that a privacy breach or suspected privacy breach requires escalation to the response team, they should co-ordinate the convening of the response team, ideally on the same working day. The response team should be convened with members meeting in person or via secure online systems (e.g. MS Teams).

The membership of a response team will always include the privacy officer that is leading the investigation. Other membership of the response team will vary depending on the incident being investigated and that membership will be determined by the privacy officer in consultation with the officer and manager that have escalated the matter. Consultation may also be undertaken with the relevant general manager and/or the Chief Executive. Typical members of a response team may include legal, communications, knowledge management, and the corresponding operational business team that relates to the suspected or actual breach.

The checklist below sets out the steps that the response team will take:

> conduct initial investigation, and collect information about the breach promptly

> determine whether the context of the information is important

> establish the cause and extent of the breach

> assess priorities and risks based on what is known

> determine who needs to be made aware of the breach (internally, and potentially externally) at this preliminary stage.

6.2 CONSIDER WHETHER THE BREACH IS NOTIFIABLE

It is the Privacy Officer's role to determine whether the breach constitutes a notifiable breach. This decision may be informed by the views of the response team. However, QLDC will always take a more cautious approach and act in favour of notifying and doing so in a timely manner.

If the Privacy Officer determines that the breach is a notifiable breach, they and the response team must co-ordinate notifications required under the Privacy Act 2020 and in accordance with best practice from the Commission. Note, that the Commission's expectation is that a breach notification should be made to its office no later than 72 hours after agencies are aware of a notifiable privacy breach. If there are reasonable grounds to believe an eligible breach has occurred, QLDC must promptly notify any individual(s) at risk of serious harm and notify the Commission using the NotifyUs[5] form on the Commission's website.

An eligible breach occurs when the following criteria are met:

> There is unauthorised access to or disclosure of personal information held by an organisation or agency (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).

> This is likely to result in serious harm to any of the individuals to whom the information relates.

> The organisation or agency has been unable to prevent the likely risk of serious harm with remedial action.

[5] https://privacy.org.nz/responsibilities/privacy-breaches/notify-us/

6.3 CONSIDER WHETHER OTHERS SHOULD BE NOTIFIED

The Privacy Officer and/or response team should consider whether others should be notified, including (but not limited to):

> Police / law enforcement,

> Other agencies or organisations that:

- May be affected by the breach, or
- Can assist in containing the breach, or
- Can assist individuals affected by the breach, or

> Where QLDC is contractually required or required under the terms of an MOU or similar obligation to notify specific parties.

7 STEP 5: REVIEW THE INCIDENT AND TAKE ACTION TO PREVENT FUTURE BREACHES

Following breaches, in cases where the Privacy Officer has not convened the response team, they together with the relevant manager and officer will undertake a post breach review and draft a report outlining the cause of the breach, implementing any strategies to identify and address any weaknesses in information handling that may have contributed to the breach, and making appropriate changes to policies and procedures if necessary.

In cases where the Privacy Officer has convened the response team, the response team should conduct a post-breach review (and draft a report) assessing QLDC's response to the breach and the effectiveness of this breach response plan. The review should consider:

> the full investigation of the cause of the breach

> implementing a strategy to identify and address any weaknesses in information handling that contributed to the breach

> updating breach response plan if necessary

> making appropriate changes to policies and procedures if necessary

> revising staff training practices if necessary

> considering the option of an audit to ensure necessary outcomes are affected

> considering whether the response team needs other expertise

> the preservation of evidence to determine the cause of the breach or allowing QLDC to take appropriate corrective action

> a communications or media strategy to manage public expectations and media interest.

The post-breach review report to be drafted by response team members should outline the above considerations, identify any weaknesses in this privacy breach response plan and include recommendations for revisions or staff training as needed. As part of the review the response team should refer to QLDCs Privacy Policy and any applicable Privacy Impact Assessment(s).

The response team should report the results of the post-breach review to QLDC's Executive Leadership Team either via email or at an Executive Leadership Team weekly meeting, depending on the severity of the incident.

7.1 TESTING THIS PLAN

Members of the response team should test this plan with a hypothetical privacy breach at least annually to ensure that it

is effective. As with the post-breach review following an actual privacy breach, the response team must report to the Executive Leadership Team on the outcome of the test(s) and make any recommendations for improving the privacy breach response plan. The test and its findings should also be referenced in the annual privacy officers' report to the Audit, Finance & Risk Committee.

8 ROLES AND RESPONSIBILITIES

POSITION	RESPONSIBILITIES
Privacy officers	**Planning for a privacy breach** - Lead the preparation, drafting and adoption of the incident response plan. - Facilitate table-top exercises to test the effectiveness of the incident response plan. - Lead organisational capability-building initiatives regarding compliance with privacy policies and legislation. **During a privacy breach** - Assist with assessing the privacy impact and risks associated with the incident. - Convening and forming the core of a privacy response team with supporting officers from relevant parts of the organisation. - Contribute to decisions regarding engagement with key stakeholders, including the Officer of the Privacy Commissioner and affected individuals.
Knowledge Management	**During a privacy breach** - Address privacy breaches and carry out forensic investigations
Legal	**Planning for a privacy beach** - Review the incident response plan to ensure it complies with all applicable legislation and policy. **During a privacy breach** - Assist with any legal issues and queries associated with the incident
Communications	**Planning for a privacy breach** - Contribute to the drafting of prepared key messages addressing a range of potential incidents that can be adapted for different stakeholders. - Develop a communications plan that includes how to manage media and public enquiries. **During a privacy breach** - Implement the communications plan and undertake any actions specific to the response. - Address media and public enquiries. - Amend and publish prepared key messages for different stakeholders

POSITION	RESPONSIBILITIES
Risk and Compliance	**Planning for a privacy breach** - Ensure the incident response plan is consistent with the Council's risk management approach and policy. **During a privacy breach** - Assist with assessing the privacy impact and risks associated with the incident
Service deliver / operations	**During a privacy breach** - Ensure the response team has access to the resources required to appropriately manage the response.
Executive Leadership Team	**Planning for a privacy breach** - Review and approve the incident plan. **During a privacy breach** - Ensure the response team has access to the resources required to appropriately manage the response. - Publicly comment on the privacy incident when required.

9 PRIVACY BREACH CHECKLIST

9.1 STEP 1: IDENITY THE BREACH (QLDC OFFICER)

Record and advise your manager of the following:

> the time and date the suspected breach was discovered

> the type of personal information involved

> the type of personal information involved

> the context of the affected information and the breach.

9.2 STEP 2: CONTAIN THE BREACH (QLDC OFFICER / DIRECT MANAGER)

> Understand and assess the breach, or suspected breach.

> Co-ordinate any action required to contain the breach.

> Notify a Privacy Officer about the breach.

9.3 STEP 3: ASSESS THE RISKS FOR INDIVIDUALS ASSOCIATED WITH THE BREACH (PRIVACY OFFICER)

- Conduct initial investigation to establish the cause and extent of the breach.
- Assess priorities and risks based on what is known.
- Notify QLDC Executive Leadership Team about the privacy breach.
- Keep appropriate records of the suspected breach including any action taken.

9.4 STEP 4: CONSIDER BREACH NOTIFICATION AND CONVENE RESPONSE TEAM

- Determine who needs to be made aware of the breach at this preliminary stage.
- Determine whether and how to notify affected individuals.
- Determine whether to escalate the breach to the response team.
- Convene the response team, if necessary.
- Determine whether the breach is an eligible breach under the Privacy Act.
- Notify the Office of the Privacy Commissioner of the notifiable breach, if necessary.

9.5 STEP 5: REVIEW THE INCIDENT AND TAKE ACTION TO PREVENT FUTURE BREACHES

- Fully investigate the cause of the breach.
- Implement a strategy to identify and address any weaknesses in QLDC information handling.
- Conduct a post-breach review and report to QLDC Executive Leadership Team on outcomes and recommendations.