



Breach of Privacy



Privacy breaches are taken seriously."

Intent

We respond quickly and proportionately to a breach of privacy. We aim to contain and mitigate the impacts and identify and address the cause(s). We notify affected people and the Privacy Commissioner if serious harm is caused or is likely to be caused and act to prevent future privacy breaches.

Responsibilities

The board will oversee and support the management of privacy risks including the actual and likely impacts of privacy breaches.

Management will:

- manage the risks and impacts of privacy breaches including notifiable privacy breaches
- consult with and report to the board about notifiable privacy breaches and any significant privacy risks
- ensure kaimahi are trained in and able to implement this policy if a breach occurs
- ensure notifiable privacy breaches are notified to the Privacy Commissioner and affected individuals in accordance with the law.



Kaimahi and volunteers will report all breaches of privacy to management including minor breaches and comply with this policy if there is a breach of privacy.

Definition

"Notifiable privacy breach" is a privacy breach that poses a risk of serious harm or causes serious harm to a person.

"Privacy breach" or "breach" involves access to or collection, use, or disclosure of personal information in contravention of our policies and the law. It may involve deliberation, deception or occur by mistake or without fault.

Requirements

Containment

If a privacy breach occurs, we will take immediate steps to contain the breach, such as:

- shutting down the [breach] activity
- revoking or changing access codes
- correcting weakness in operational or electronic security.

Review for cause and impact

A preliminary review will be undertaken to identify the cause of the breach, scope the extent of it and assess the impacts on the individuals whose information it is.

Further steps to contain and manage the breach will be taken if indicated by this review.

Evidence of the breach will not be destroyed until the investigation is completed.

Notifying the Privacy Commissioner and affected individuals



Unless a [legal exception](#) applies, the Privacy Commissioner and affected individuals will be notified of the privacy breach if it has caused or is likely to cause serious harm having regard to:

- the extent to which our response to the breach has reduced the harm/risk of harm
- who is likely to receive the information as a result of the breach
- the sensitivity of the information to the individual whose information it is
- whether the information is protected by a security measure
- other relevant matters.

The [NotifyUs tool](#) will be used to help decide if a privacy breach should be notified. If we are unsure if serious harm has been caused or may be caused by a breach, management/their delegate will notify the Privacy Commissioner and be guided by their advice.

Notifications will:

- be made as soon as reasonably practicable after the privacy breach
- cover the following:
 - when and how the breach occurred
 - the nature and scope of personal information
 - what we've done to control or reduce the harm
 - people/agencies who have been informed about the breach
 - other relevant matters.
- be made to the Privacy Commissioner [here](#).

In addition to the above, affected individuals will be informed (eg through email, phone or in-person meeting) about the following:

- what they can do to avoid or reduce harmful impacts and to further protect themselves
- that we have notified the Privacy Commissioner
- their right to make a complaint using our internal complaints process and to the Office of the Privacy Commissioner



- how they can contact us
- the identity of the recipient of the personal information if the disclosure is necessary for safety reasons.

Public notifications

If it is not reasonably practicable to notify individuals who are or may be affected by the privacy breach and [no legal exception applies](#), we will give public notice about the privacy breach (eg on our website etc).

Informing others

The following will also be informed of the privacy breach on as-needed basis:

- the board for all notifiable breaches and any breach posing a significant risk to the organisation
- the Police, if criminal activity appears to be involved
- any person who can assist with containing and lessening the impacts of the breach
- if relevant, our insurer
- any regulatory or professional membership organisation (if the breach involved misconduct or negligence by staff.)

Prevention

We will investigate any privacy breach, including minor breaches, to the extent necessary to ascertain:

- the cause of the breach and
- what controls are needed to prevent a future breach.

Both the investigation and controls should be proportionate to the significance of the privacy breach. The risk of future breach and the efficacy of the controls will be monitored in accordance with our [risk management](#) and [quality improvement](#) approach.

Recordkeeping



We will be transparent about how we respond to and manage privacy breaches by ensuring that we record the steps we take and our reasoning. This will include recording our reasons for deciding to report or not report a privacy breach to the Privacy Commissioner and affected persons.

Helpful links

[Sharing information without consent](#)

[Safeguarding personal information](#)

[Notify us \(Privacy Commissioner's self assessment tool\)](#)

Review

Date: October 2020

Next review: by September 2022