Authorised Policy of Methodist Mission Southern ("the Methodist Mission")

P9.2.3 : Privacy Officer, Requests, and Breaches

Policy

PRIVACY OFFICER

For the purposes of Section 23 of the Privacy Act (and any amendments to it) the Privacy Officer for the Mission is the Kaihautū Director. The role of the Privacy Officer is to:

- Encourage compliance with the Information Privacy Principles and with other provisions of the Privacy Act;
- Deal with requests for personal information and issues concerning personal information generally;
- Ensure all reporting of Privacy Breaches are notified to the appropriate agencies;
- Work with the Privacy Commissioner when s/he is investigating complaints of "interference with privacy" where an individual has claimed that one has been caused by the agency.

PRIVACY ACT REQUESTS

It is noted that requests for information may include (but not be limited to): CCTV footage, hard copy documents, electronic documents, emails, voicemail messages, recorded video conference meetings, and SMS (texts).

Requests by employees or others for personal information (as provided for under the Privacy Act 1993) may be forwarded through their Manager, or direct to any employee authorised to handle such enquires.

Requests from individuals or statutory agencies, such as Police or CYFS, under the Act's exemption for "maintenance of the law" will be declined without:

- That agency certifying (preferably in writing) that their request meets the requirements of the Children's Act, or
- A Production Order or Warrant being provided in advance, or
- The requirements of the Mission's Policy for At Risk Clients (P7.17) being met, or
- The agency certifying that the request meets the tests of Principle 11 e(iv) or Principle 11 f(ii) of the Act which allow for acting in situations of concern for the health and wellbeing of the client.

PRIVACY ACT PRINCIPLES

The Principles of the Privacy Act may be viewed on the website of the Privacy Commissioner, at http://www.privacy.org.nz/a-thumbnail-sketch-of-the-privacy-principles/.

OFFICIAL INFORMATION ACT REQUESTS

Information held by the Mission that has been gathered in order to meet the expectations of a contract with a government organisation may be subject to the Official Information Act via that agency.

Requests for access to that information under the Official Information Act should be made or referred to the government organisation under which contract it has been gathered. That organisation may then request of it from the Mission under the terms and conditions of their contract with us.

Otherwise the Mission is not subject to the provisions of the Official Information Act. Requests for information made by persons about themselves or minors for whom they are the legal guardian quoting the Official Information Act will be treated as if they were being made under the provisions of the Privacy Act.

PRIVACY BREACHES
Breaches are defined by the harm or potential harm that is / could be created. This will always be a factor of the volume of people involved as well as the amount and nature of individual information released.

DEFINITIONS
Harm is damage or injury experienced by an individual person e.g. a client of the Mission or an employee of the Mission in their identity as a private person.

Low levels of harm are those that are not disruptive to a person's life or their experience of their life. Regardless of the impact on those who's privacy has been breached, this kind of harm gives the lie to the Mission's stated commitment to observing and protecting the privacy of those whose private information we hold. Low levels of harm therefore still carry a potential for harm to the Mission's reputation.

Moderate levels of harm are those that may be disruptive to a person's life or their experience of their life, or are otherwise low or medium level harm but involve more than one or two individuals or a single whānau, and / or involve investigation or oversight by the Office of the Privacy Commissioner or any other accreditation, regulatory, or funding body.

High levels of harm are those that are significantly disruptive to a person's life or their experience of their life, or are otherwise low or medium level harm but involve a large number of people, are maliciously undertaken or for the personal benefit of a staff member, or for other reasons create significant risk of damaging the Mission's reputation, accreditations, or funding arrangements.

Individuals concerned are the people whose privacy is breached. These may include clients, associates or relatives of clients (i.e. where information provided by a client about other persons in their life), and staff.

Privacy breach occurs when private and identifiable information on one or more persons held by the Mission is released to other persons outside the Mission, or accessed by unauthorised individuals within the Mission for their own benefit, without the individual(s) concerned's consent, and otherwise outside of the provisions of the law, e.g. reporting of at risk children to Oranga Tamariki, reporting of at risk of family violence of child abuse to Police, reporting of criminal behaviour by a staff member, reporting of those at risk of self-harm to Emergency Psychiatric Services, as required by professional bodies (e.g. Education Council), or as part of the Mission's accreditation or funding agreements (i.e. quality audits), or as demanded by a production order.

This information maybe on a relative or associate of a client and they may not be aware that the Mission holds that information. Additional care is required when this information is the subject of a privacy breach.

A breach may also be caused by an unauthorised individual or group maliciously accessing Mission files e.g. burglary or theft of Mission devices, by the loss or misplacement of Mission devices, or by hackers penetrating the Mission's IT system.

Support may range from counselling to financial assistance, to full mitigation of costs incurred to resolve the disruption to the individual(s) concerned(s)' life.

RESPONDING TO A BREACH
The four steps in of responding to a breach or suspected breach are:

1. Breach containment and preliminary assessment;
2. Evaluation of the risks associated with the breach;
3. Notification; and
4. Prevention.

Breach Containing and Preliminary Assessment
While the Mission's IT system has previously come under attack from a hacker, it is expected that the bulk of our breaches will be inadvertent: sending an email containing private information to the wrong person, misplacing or having stolen a digital device holding client or staff private information, sharing insufficiently "anonymised" information with a third party that is able to be or is re-identified.

Evaluation of the harm associated with the breach
The Mission holds sensitive information on clients, associates of clients, and employees. Their interests may diverge, and their resiliency (or the amount they might care) about private information being shared will depend on both personal circumstances, who the information was inappropriately shared with, and the nature of the information released.

Notification
The responsibility is to notify not only those whose information has been inappropriately accessed or shared, but also the Mission's liability insurer (per MCNZ Lawbook), and potentially the Office of the Privacy Commissioner. If the breach is criminal, Police will be notified, if the breach is financial (e.g. records of families paying for ECE) then banks may need to be advised etc. If the breach is in regard to the Mission's Early Learning Centre(s) and notification is made to the Office of the Privacy Commissioner, then notification will also be made to the Ministry of Education.

Notifications to the Office of the Privacy Commissioner **must** be made for Moderate and High Harm breaches and **must** be made within 72 hours of the Mission being aware of the breach occurring.

Prevention
Following an investigation, it is possible that changes to Mission practice, IT systems and security, or other elements of the way we maintain client and employee privacy will be required. It is also possible that disciplinary action may be appropriate. Investigations will be undertaken as soon as possible by the Kaihautū and Kaiārahi Hakarau Pāroko Chief Advisor Data jointly.

SHORT GUIDE
This guide is not exhaustive but indicative:

Type	Low	Moderate	High	Who
Report to Line Manager ***before*** responding	----------Mandatory----------			All staff
Report to the Mission's Privacy Officer (MPO) (aka the Mission's Director)	----------Mandatory----------			All staff
Treat as a "complaint" for investigation under Mission complaints policy	----------Mandatory----------			All staff
Record in Privacy Breaches Register	----------Mandatory----------			MPO
Notify liability insurer	Consider	Mandatory	Mandatory	Director
Notify the Office of the Privacy Commissioner	Consider	Mandatory	Mandatory	MPO, ICT Leader
Notify Ministry of Education (if OPC)	Consider	Mandatory	Mandatory	MPO, ICT Leader
Where an inadvertent sharing, retract as soon as possible (see below)	----------Mandatory----------			All staff or MPO
Advise individual(s) concerned(s), in person if possible	Advised	----------Mandatory----------		Practice Leader or Director
Provide individual(s) concerned(s) with access to support	Preferable	----------Mandatory----------		Practice Leader or Director
Address individual(s) concerned requests for remediation / response	Consider	Advised	Mandatory	Practice Leader or Director
Remote wipe any stolen or misplaced devices	----------Mandatory----------			ICT Leader
Report to police any stolen or misplaced papers	Advised	----------Mandatory----------		Practice Leader or Director

or devices			
Incident review	Advised	----------Mandatory----------	MPO
Undertake disciplinary investigation where breach is malicious, repeated, significant		---------- Consider ----------	Director

Please note: Disciplinary investigations do not always lead to misconduct findings, and misconduct findings do not always lead to sanctions (which range from verbal through to final written warnings, and termination). It is expected that termination would only be an option should an employee have acted maliciously, where the breach had put lives at risk, where the breach had created a risk of threat to Mission contracts and/or services, or who had created multiple or repeated privacy breaches.

RETRACTIONS
Suggested retraction wording for breaches via email. To be sent marked "important".

Subject: URGENT: Email Sent In Error

Please be advised that information emailed to you on ***dd/mm/yyyy*** by ***MMS staff member***, was sent in error and contains sensitive information which was not intended for you. As the email contains privileged information, we would respectfully ask that you do not discuss or disseminate its contents.

We sincerely apologise for this error, and request that you delete and/or destroy the original email and any digital/physical copies from your systems.

As we maintain an internal privacy breach register, we would appreciate it if you could reply to this request, to confirm that you have acknowledged and actioned the deletion of the email.

NOTIFYING A DATA BREACH TO THE PRIVACY COMMISSIONER
Include information about the incident such as:

- Information about the incident and its timing in general terms
- A description of the personal information involved in the breach
- A general account of what your agency has done to control or reduce the harm
- What your agency will do to assist individuals and steps individuals can take to reduce the risk of harm or further protect themselves
- Sources of information designed to assist individuals in protecting against identity theft
- Contact information of a department or individual within your organization who can answer questions or provide further information
- Whether your agency has notified the Office of the Privacy Commissioner
- Additional contact information to address any privacy concerns to your agency, and
- Contact information for the Office of the Privacy Commissioner.

Also Look Up

Related Policies: P4.5, P7.17, P9.21
Related Form(s):

Policy Created: 1 June 2001
Date of Last Revision: October 2022
Date of Next Review: July 2024

Authorised by:

Director