Privacy breach management

Table of Contents

Policy statement and principles

What

A privacy breach is unauthorised or accidental access to, or collection, use or disclosure of, personal information in contravention of the Privacy Act 2020. A privacy breach includes a 'near miss' - e.g. where a wrongly addressed letter is returned to Police unopened.

This chapter provides examples of privacy breaches and outlines the steps for responding.

Why

In the event of a privacy breach, whether it is a serious or minor incident, managing it appropriately will assist Police in retaining the trust of affected individuals and the public. Where poorly handled, the damage to individuals as well as the public's trust and confidence in Police, can be serious and irreparable.

How

- Privacy breaches must be contained immediately.
- Police ICT will provide direction if the incident involves information technology.
- All privacy breaches must be reported on the Security and Privacy Incident Register with direct reporting also to the District Operations Manager or Chief Privacy Officer, PNHQ, in urgent situations.
- Risks associated with breaches are assessed and affected individuals and the Privacy Commissioner are notified of the breach where necessary. The Data Breach Severity Report tool is used to help with assessments.
- Police will consider advising others apart from the individual concerned in serious incidents, or when the matter is likely to be made public.
- Breaches are investigated after the risks are mitigated and prevention plans developed when appropriate.

Overview

Purpose

This chapter details the 4 steps to take when responding to a privacy breach. The steps include recording the breach on the in the Security and Privacy Incident Register (SPIR) tool, for the purpose of national oversight, mandatory reporting to the Privacy Commissioner and statistical reporting.

What is a privacy breach?

A privacy breach is unauthorised or accidental access to, or collection, use or disclosure of, personal information in contravention of the Privacy Act 2020. A privacy breach includes a 'near miss' - e.g. where a wrongly addressed letter is returned to Police unopened.

Examples of privacy breaches

Some examples of privacy breaches include:

- releasing personal information to the wrong person, e.g. by sending it to the wrong physical or email address, or wrongly including information about a third person
- laptops, removable storage devices, or physical files containing personal information being lost or stolen or insecurely disposed of
- Police databases containing personal information being hacked into or otherwise illegally accessed by outsiders
- individuals deceiving Police into improperly releasing the personal information of another
- employees accessing personal information outside of the requirements of their employment
- failing to release or correct information as required by the Privacy Act 2020.

Related information

This policy is largely based on the guidelines published by the Privacy Commissioner.

The Office of the Privacy Commissioner's website also has many other helpful resources relating to information privacy, disclosure, information loss and privacy breaches. Follow this link to their 'Guidance resources'.

Related Police Manual chapters

See also these Police Manual chapters (or parts):

- Privacy and official information:
  - Disclosure under the Privacy Act 2020
  - Disclosure under the Official Information Act 1982 (OIA)
  - Applying the Criminal Records (Clean Slate) Act 2004
- Criminal disclosure
- Departmental security:
  - Personnel security

    - Employee telephone requests for information

- Information security and assurance:

    - Information security for guidance about Police employees preserving personal privacy

    - Inappropriate access, use and procurement

    - Electronic redaction and disclosure for how to securely remove parts of information being provided electronically to protect privacy and confidentiality and/or to comply with legislation and Police policy

Steps for responding to privacy breaches

Introduction

Move immediately to investigate any actual, suspected or potential breach and its potential for harm, including whether notification to the Privacy Commissioner and affected individual is required.

All privacy breaches or incidents must be reported on the the Security and Privacy Incident Register (SPIR) notification. The SPIR system will notify your nominated supervisor, who will nominate the District Operations Manager/Director. An automatic notification will also be directed to the Chief Privacy Officer at PNHQ and, if there are security implications, the Manager: Protective Security.

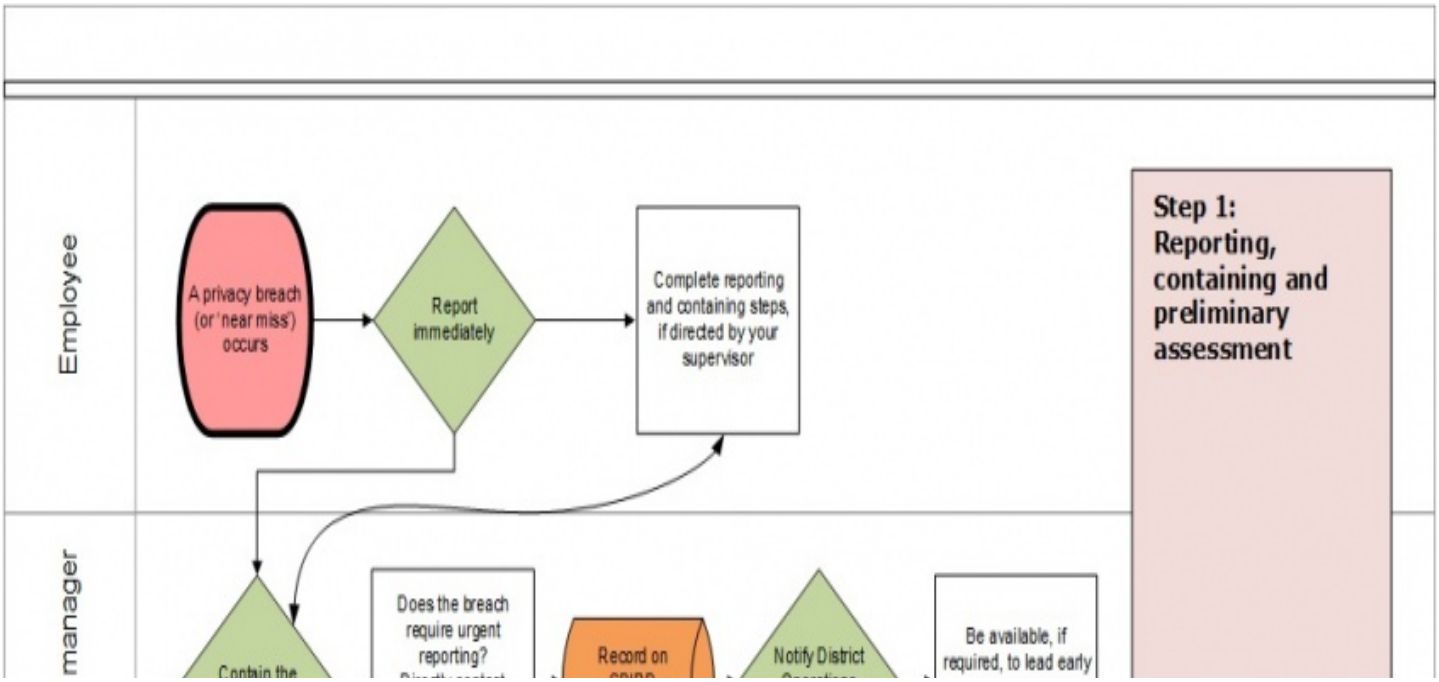
Four steps to take in response to a privacy breach

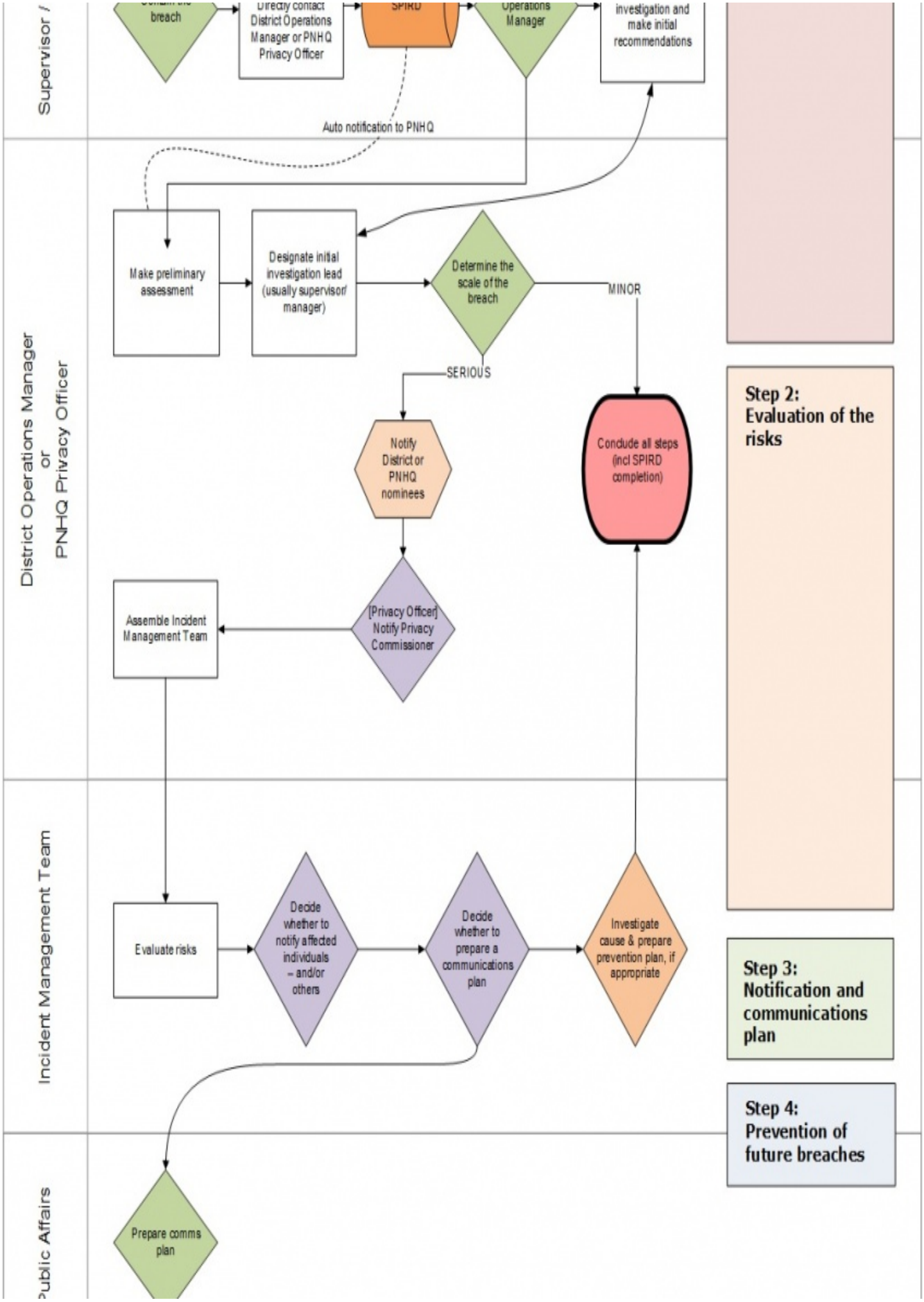
There are four key steps in responding to a privacy breach:

Step	Description
1	Reporting, containing and preliminary assessment of the breach
2	Evaluation of the risks associated with the breach
3	Notification to the Privacy Commissioner and affected individuals if necessary
4	Prevention of future breaches

Steps 1, 2 and 3 should be undertaken either simultaneously or in quick succession. Step 4 provides recommendations for longer-term solutions and prevention strategies. Not all steps may be necessary, or some steps may be combined.

Overview of the privacy breach management process





Step 1: Reporting, containing and preliminary assessment of breach

Police employee action

If you are aware of an actual, suspected or potential privacy breach or 'near miss', report the incident to your supervisor/manager immediately.

If directed by your supervisor/manager, or if you are a supervisor/manager, complete the following action yourself.

Supervisor/manager action

The supervisor/manager must follow these steps to limit damage and report the breach:

Step	Action
1	Contain the breach immediately, e.g: - recover the personal information from the unintended recipient by contacting them and seeking their cooperation to delete or return any electronic or hard copy information - stop the unauthorised practice - shut down the system that was breached - revoke or change computer access codes or correct weaknesses in physical or electronic security. **Note:** If the incident involves information technology, seek direction from the PoliceICT Service Desk before taking any containment steps.
2	Record the breach as soon as practicable (after containing the breach and addressing any urgent safety concerns) on the Security and Privacy Incident Register (SPIR). - Include a full incident description, including: - What was the date of the incident? - When was the incident discovered? - How was it discovered? - What was the location of the incident? - What was the nature and extent of the privacy breach? - What was the cause of the incident? - Have you contained the breach? SPIR notification will trigger automatic notification to the Chief Privacy Officer atPNHQ. For District incidents, notify the District Operations Manager. If you consider the privacy breach requires urgent reporting, directly contact: - District Operations Manager, or - Chief Privacy Officer to alert them early to the incident before recording it on SPIR.
3	Be available to assist the District Operations Manager orPNHQ Chief Privacy Officer. If required, lead the early investigation and make initial recommendations.

District Operations Manager or PNHQ Chief Privacy Officer action

The District Operations Manager orPNHQ Chief Privacy Officer must:

Step	Action

Step	Action
1	Review the incident report details, focussing on the: - nature, sensitivity, volume, impact, categorisation and risk rating of incident - containment measures taken and potential resolution of the incident - effectiveness of the initial incident response to immediately assess the risk, emerging priorities and next steps.

2	Make a preliminary assessment of the breach, considering factors such as:
	
	- single or multiple breaches
	- snippet or large amount of information involved
	- single or multiple or unknown affected individuals
	- single recipient of information versus world wide web accessibility
	- effectiveness of breach containment measures
	- whether there is criminal activity involved
	- employee breach versus systems breach
	- likelihood of:
	  - harmful consequences to affected individuals
	  - litigation
	  - investigation by the Office of the Privacy Commissioner
	  - media knowledge and interest
	- risk of damage to Police reputation and citizen trust.

3	Designate an appropriate individual to lead the initial investigation and make initial recommendations. This will usually be the supervisor/manager who reported the breach as they are closely associated with the events.
4	Consider the results and recommendations of the initial investigation, your preliminary assessment, and the risk evaluation (see Step 2) to determine whether: - the breach is minor and can be or has been effectively managed; or - the breach is serious and there is a need for a more detailed investigation.
5	For minor incidents, ensure all steps are concluded, including: - notifying affected individuals, where considered appropriate (see Step 3), and - taking appropriate steps to prevent future breaches (see Step 4); and complete the breach report in SPIR.
6	For serious incidents, notify: - District: Area Commander/designated Inspector or District Commander - PNHQ - Director: Assurance

Step	Action
7	For serious privacy breaches, assemble an Incident Management Team.

Incident Management Teams

If an Incident Management Team is to be assembled, consider including:

- District Operations Manager and/or PNHQ Chief Privacy Officer and/or Manager: Protective Security/Chief Information Security Officer
- Supervisor/manager of employee involved with the breach
- District or PNHQ Legal Adviser
- District or PNHQ HR Adviser
- District or PNHQ Integrity and Conduct Manager
- PNHQ Media Adviser
- ICT representative (if subject matter expert is required)
- Other subject matter experts as appropriate (internal or external, for example, IT analysts or risk advisers).

Step 2: Evaluation of the risks

To determine what other steps are immediately necessary, the District Operations Manager orPNHQ Chief Privacy Officer, or Incident Management Team (if assembled), must assess the risks associated with the breach.

Use the Data Breach Severity Report tool (*see PDF below*) to assist with your evaluation of the risks and consider these factors:

1	Consider what personal information was involved.
2	Establish the cause and extent of the breach.
3	Consider who is affected by the breach.
4	Identify whether harm could foreseeably result from the breach.
Keep a record of the Data Breach Severity Report.	

Consider what personal information was involved

To consider what personal information was involved, ask these questions:

Step	Question/description
1	What is the precise extent of personal information involved in the breach?
2	How sensitive is the information? For example: - victim information - confidential/informant/witness information - criminal history - health information - driver licence numbers Some personal information is more sensitive than other information. Generally, the more sensitive the information the higher the risk of harm to individuals. A combination of personal information is typically more sensitive than a single piece of personal information. However, sensitivity is just one consideration when assessing the risk.
3	What is the context of the personal information involved? For example, a list of people spoken to by Police may not be sensitive. However, the same information about those people where there was an express or implied expectation of confidentiality due to the nature of the Police investigation is more sensitive. Similarly, publicly available information such as Police evidence given at trial and already reported in the media is less sensitive.
4	Is the personal information adequately encrypted, anonymised, or otherwise inaccessible?
5	How can the personal information be used? Can the information be used for fraudulent or otherwise harmful purposes? The combination of certain types of sensitive personal information along with name, address and date of birth suggest a higher risk due to the potential for identity theft.

Note: An assessment of the type of personal information involved will help the District Operations Manager, PNHQ Chief Privacy Officer or Incident Management Team, to determine how to respond to the breach, who is required to be informed, including the Office of the Privacy Commissioner, and what form of notification to the individuals affected, if any, is appropriate. For example, if a laptop containing adequately encrypted information is stolen, quickly recovered and investigations show that the information was not tampered with, notification to individuals whose information was contained on the laptop will not be necessary.

Establish the cause and extent of the breach

Establish the cause and extent of the breach by answering these questions:

Step	Question
1	To the extent possible, can you determine the cause of the breach?
2	Is there a risk of ongoing breaches or further exposure of the information?
3	What was the extent of the unauthorised access to or collection, use or disclosure of personal information, including the number and nature of likely recipients and the risk of further access, use or disclosure, including via mass media or on-line?
4	Was the information lost or was it stolen? If it was stolen, can it be determined whether the information was the target of the theft?
5	Has the personal information been recovered?
6	What steps have already been taken to mitigate the harm?
7	Is this a systemic problem or an isolated incident?

Consider who is affected by the breach

Consider who is affected by the breach by answering these questions:

Step	Question
1	How many individuals were affected by the breach?
2	Who is affected by the breach, e.g. employees, service providers, the public, victims, informants, witnesses?

Identify whether harm could foreseeably result from the breach

To identify whether harm could foreseeably result from the breach, consider the reasonable expectations of the individuals affected and ask these questions:

Step	Question/description
1	Who is the recipient of the information?
2	Is there any relationship between the unauthorised recipients and the affected individual? For example: Was the disclosure to an unknown party or to a party suspected of being involved in criminal activity where there is a potential risk of misuse? or Was the recipient a trusted, known entity or person that would reasonably be expected to return the information without disclosing or using it?
3	What harm to the affected individual could result from the breach? Examples include: - security risk, e.g. physical safety - identity theft - financial loss - loss of business or employment opportunities - significant humiliation or loss of dignity, damage to reputation or relationships.
4	What harm to Police could result from the breach? Examples include: - compromise of criminal investigation - loss of trust and confidence in Police - damage to reputation - loss of assets - financial exposure - legal proceedings.
5	What harm could come to the public as a result of the breach? An example of harm that could result is a risk to public safety, or a significant loss of trust and confidence in an important public service.

Step 3: Notification and communications plan

Overview of notification considerations

Notification can be an important mitigation strategy that has the potential to benefit both the agency and the individuals affected by the breach. If a privacy breach creates a risk of harm to the individual, those affected should usually be notified. Where serious harm is evident or there is a likelihood of serious harm to individuals (termed a 'notifiable breach') both the individuals and the Privacy Commissioner must be advised. (See Deciding whether to notify affected individuals below). Prompt notification to individuals in these cases can help them mitigate the damage by taking steps to protect themselves. Notifying the Privacy Commissioner and affected individuals must be completed as soon as practicable.

Each incident needs to be considered on a case-by-case basis to determine whether privacy breach notification is necessary. It is important to be certain of whose information has been affected because more damage can be done if the wrong people are notified.

The key consideration in deciding whether to notify affected individuals, is where the breach has caused or is likely to cause serious harm. Notification to individuals may enable them to avoid or mitigate harm where personal information has been inappropriately accessed, collected, used or disclosed. Even where the individual cannot take any steps to mitigate potential harm, the privacy breach may be so serious as to warrant notification.

Overview of communications plan

Where the incident is serious or likely to be made public, it may also be advisable to notify others apart from the individual concerned and to develop a communications plan. The Chief Privacy Officer at PNHQ will inform the Office of the Privacy Commissioner about serious privacy breaches as required by the mandatory reporting provisions of the Privacy Act 2020 so they can effectively handle any related enquiries or complaints. Media and Communications Group at PNHQ will manage or be available to advise on any communications plan.

Making decisions on notification

The following steps ought to be considered when deciding whether or not to notify affected individuals and if so, when and how:

	Matters for consideration
1	Deciding whether to notify affected individuals
2	When to notify, how to notify and who should notify
3	What should be included in the notification
4	Others to contact
5	Communications plan

Deciding whether to notify affected individuals

Consider these factors when deciding whether to notify:

Step	Factors for consideration
1	What are the legal and contractual obligations?
2	What actions have been taken by Police to reduce the risk of harm following the breach?
3	Is the information sensitive?
4	Is the information protected by a security measure?
5	What is the risk of harm to the individual?
6	Is the person or agency who has obtained the information trustworthy or not?
7	Is there a risk of identity theft or fraud (usually because of the type of information lost, such as an individual's name and address together with government-issued identification numbers or date of birth)?
8	Is there a risk of physical harm (if the loss puts an individual at risk of physical harm, stalking or harassment)?
9	Is there a risk of significant humiliation, embarrassment, loss of dignity, or damage to the individual's reputation or relationships. For example, when the information lost includes employee medical or disciplinary records, criminal/traffic convictions, informant details, sensitive victim information, or health/family violence/offending alerts?
10	What is the ability of the individual to avoid or mitigate possible harm?
11	Is notifying the individual likely to cause distress or alarm, particularly where the above risks are low?

When to notify, how to notify and who should notify

At this stage, compile as complete a set of facts as possible including a risk assessment in order to determine whether to notify individuals. Use of the Data Breach Severity Report tool will assist this assessment.

-

Data Breach Severity Report Tool.docx	**37.74 KB**

When to notify

Individuals affected by the breach should be notified as soon as practicable following assessment and evaluation of the breach. However, it may be necessary to delay notification to ensure that an investigation is not compromised.

How to notify

Notification may be direct or indirect:

Direct notification	The preferred method of notification is direct - by phone, letter, email or in person - to affected individuals.
Indirect notification **(Senior Manager approval required)** **Note**: Senior Manager in this context includes: - Commissioner, Deputy Commissioner, Deputy Chief Executive or Assistant Commissioner - District Commander - Executive Director or Director.	Notification that needs to be indirect - website information, posted notices, media - should generally only occur where direct notification is not reasonably practicable because it could cause further harm to the individuals or may prejudice public interests such national security or law enforcement. Other factors may include the cost of notification is prohibitive , or the contact information for affected individuals is not known. Using multiple methods of notification may be appropriate. Also consider whether the method of notification might increase the risk of harm, for example, by alerting the person who stole the laptop to the value of the information it contains. Indirect notification must be authorised by a senior manager.

Who should notify?

The District Operations Manager, PNHQ Chief Privacy Officer, or Incident Management Team (if assembled) will determine the most appropriate person to notify individuals affected, depending on the nature of the breach.

PNHQ's Chief Privacy Officer will ordinarily manage the notification to the Office of the Privacy Commissioner. Alternatively, the Director: Assurance can perform this function.

Police should make the notification where the breach occurs by a third-party service provider contracted to Police to maintain or process the personal information which is the subject of the breach.

What should be included in the notification?

Affected Individuals

The content of notifications will vary depending on the particular breach and the method of notification chosen. Notifications must include:

- A description of the breach including the nature of information at risk
- Advice about whether we know who has the information without identifying that person or agency unless identifying that entity is necessary to prevent or lessen a serious threat to the life or health of the affected individual or another person
- An explanation of the steps we have taken and will take to respond to the breach including what we have done to control or reduce harm
- Advice to the individual about steps they may wish to take to avoid or reduce harm and the nature of any assistance we can provide
- Confirm that the Privacy Commissioner has been notified
- Advise the individual's right to make a complaint to the Privacy Commissioner
- Provide the individual with a contact person in Police for further inquiries.

Some useful online guidance that may assist individuals to protect themselves against identity theft can be found on the following websites:

- Police: https://www.police.govt.nz/advice-services/cybercrime-and-internet
- Consumer Protection unit of the Ministry of Business, Innovation and Employment: https://www.consumerprotection.govt.nz/general-help/scamwatch/
- CERT NZ: https://www.cert.govt.nz/individuals/
- Netsafe: http://www.netsafe.org.nz/

Be careful not to include unnecessary personal information in the notice to avoid possible further unauthorised disclosure.

Others to contact

Others to contact may include:

Office of the Privacy Commissioner	Serious privacy breaches also referred to as notifiable breaches must be reported to the Office of the Privacy Commissioner as this will help that Office respond to inquiries made by the public and any complaints received. The Office of the Privacy Commissioner may also be able to provide advice or guidance in responding to the breach. Failure to advise the Privacy Commissioner of a notifiable breach is an offence and liable to a fine up to $10,000. **Note:** The Chief Privacy Officer at PNHQ must be used to inform the Office of the Privacy Commissioner (alternatively, channel through the Director: Assurance). The Privacy Commissioner will be informed of: - the nature of the breach including the number of affected individuals and the identity of the person or agency in possession of the affected personal information - the steps Police has taken or will take in response to the breach - whether or not the affected individuals have been advised - whether advise is directly to individuals and if not the reasons why - the other agencies that have been advised about the breach and why - a contact person within Police for further inquiries. Notifying the Privacy Commissioner may enhance the public's understanding of the incident and confidence that Police is taking the incident and its responsibilities seriously.
Independent Police Complaints Authority (IPCA)	If: - a complaint against Police is received under section 15 of the Independent Police Conduct Authority Act 1988 - the matter involves criminal offending or serious misconduct by a Police employee, where that matter is of such significance or public interest that it places or is likely to place the Police reputation at risk (see Police/IPCA MOU) - notification to be achieved through the District or Service Centre Police Professional Conduct Manager, for consideration, categorise the incident and where appropriate notify the Authority. See the Police investigations of complaints and notifiable incidents chapter for further information.

Other internal or external parties not already notified	- Chief Information Security Officer, at PNHQ - Government Chief Privacy Officer - National Cyber Security Centre if the incident involves unauthorised access or attempts to gain unauthorised access to a computer system or its information or unauthorised use of a system for processing or storing information. - Third party contractors or other parties who may be affected - Internal groups not previously advised of the privacy breach, for example, Media and Communications, Police Professional Conduct, or the Security and Privacy Reference Group - Police Association or Police Leaders' Guild - Office of the Minister of Police

Communications plan

If the privacy breach is serious or likely to be made public, Media and Communications Group must be consulted for assistance with preparing a communications plan and determining an approval process for internal and external communications.

The Office of the Privacy Commissioner suggests that an important rule of thumb in coping with media interest is to respond quickly to their requests. How Police deals with the story, or fails to deal with it, could become as important as the incident itself.

See also the Dealing with the media and Media interviews Police Manual chapters.

Step 4: Prevention of future breaches

Investigation

Once appropriate reporting and the immediate steps are taken to mitigate the risks associated with the breach, the District Operations Manager, PNHQ Chief Privacy Officer or Incident Management Team (if assembled) should:

- direct an investigation into the cause of the breach (if it is not already apparent)
- consider whether to develop a prevention plan.

The level of effort must reflect the significance of the breach, and whether it was a systemic breach or an isolated instance. Do not assume that there is nothing that can be done to prevent future mistakes, as there is a system failure behind many errors. Future 'one-off mistakes' may be prevented by process changes or training updates.

The objective of ensuring any privacy breach is promptly reported and properly handled is not so disciplinary action can be taken. Mistakes can be made by anyone and acknowledging them shows integrity and commitment to doing the right thing for Police and the public. However, where the cause of the breach indicates:

- a deliberate breach of the Code of Conduct, an employment investigation may be considered, or
- malicious or criminal actions, a Police investigation may be commenced.

Prevention plan

The prevention plan may include:

- a security audit of both physical and technical security
- a review of:
    - policies and procedures and any changes to reflect the lessons learned from the investigation and regularly after that, e.g. security policies, record retention and information collection policies
    - employee training practices, and
    - service delivery partners caught up in the breach.

The prevention plan may include a requirement for an audit at the end of the process to ensure that the prevention plan has been fully implemented.

Notifiable Privacy Breaches

Following the conclusion of an investigation into a notifiable privacy breach a report must be referred to the Security and Privacy Reference Group (SPRG) the governance group that has initial responsibility for managing security and personal information risks. The report must include:

- full details of the breach investigation including describing the information and the affected individuals involved

- how and when containment of the breach was achieved
- how and when affected individuals were notified of the breach including their general response to the incident
- the nature of any communications plan and how it was implemented, and
- details of any prevention plan or details of the root cause for the incident including any recommendations to avoid a repeat of the breach.

Forward final reports to the PNHQ Chief Privacy Officer who will be responsible for bringing them to the attention of the SPRG.

Printed on : 09/06/2022