Privacy breach management

Table of Contents

Table of Contents 2
Policy statement and principles 3
What 3
Why 3
How 3
Related information 3
Related Police Manual chapters 3
Privacy Breach: Response Steps (Quick guide) 4
Privacy Breach: Response Steps (Detailed steps) 5
Step 1: Contain and report 5
Step 2: Assess the impact 5
Information type and sensitivity 6
Context of information loss or disclosure 6
Status of the breach 6
Harm to Police 6
Escalation decision making 7
Step 3: Notify (and apologise) 7
Deciding whether to notify 7
When, who and how 8
What should be included in the notification? 9
Others to contact 10
Step 4: Prevent future breaches 10
Investigate root cause 10
Disciplinary steps 10
Prevention plan 10
Notifiable Privacy Breaches 10

Policy statement and principles

What

A privacy breach is an unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of personal information. It can also be an action preventing Police from accessing its own data.
Personal information is any piece of data about an identifiable person - it could be contact information, health details, criminal history records or a victim impact statement. Personal information does not necessarily need to be directly connected to a named person - a combination of details may be enough to identify an unnamed person.

Some examples of privacy breach incidents are:

- sending an email with attached spreadsheet to the wrong recipient
- unauthorised or accidental disclosure of information to another person or agency
- failure to redact witness details in a criminal disclosure pack
- accessing a NIA record without a valid business reason.

Why

Police has a responsibility under the Privacy Act 2020 to notify affected individuals and the Privacy Commissioner about privacy breach incidents that have caused, or may cause, serious harm.
When a privacy breach occurs, acting quickly to contain the situation, supporting seriously affected individuals and reporting the incident helps Police maintain the trust and confidence of affected individuals and the public.

How

Report all ‘privacy breaches' or any incident or concern involving personal information in the Security and Privacy Incident Register (SPIR) within 24 hours of becoming aware of the incident.

Once a SPIR report is submitted, the PNHQ Privacy Team will review it and may seek further details and/or provide advice to support the breach response.

The Chief Privacy Officer (CPO)/Privacy Team is responsible for notifying the Privacy Commissioner about serious privacy breaches within 72 hours of Police becoming aware of the incident.

Related information

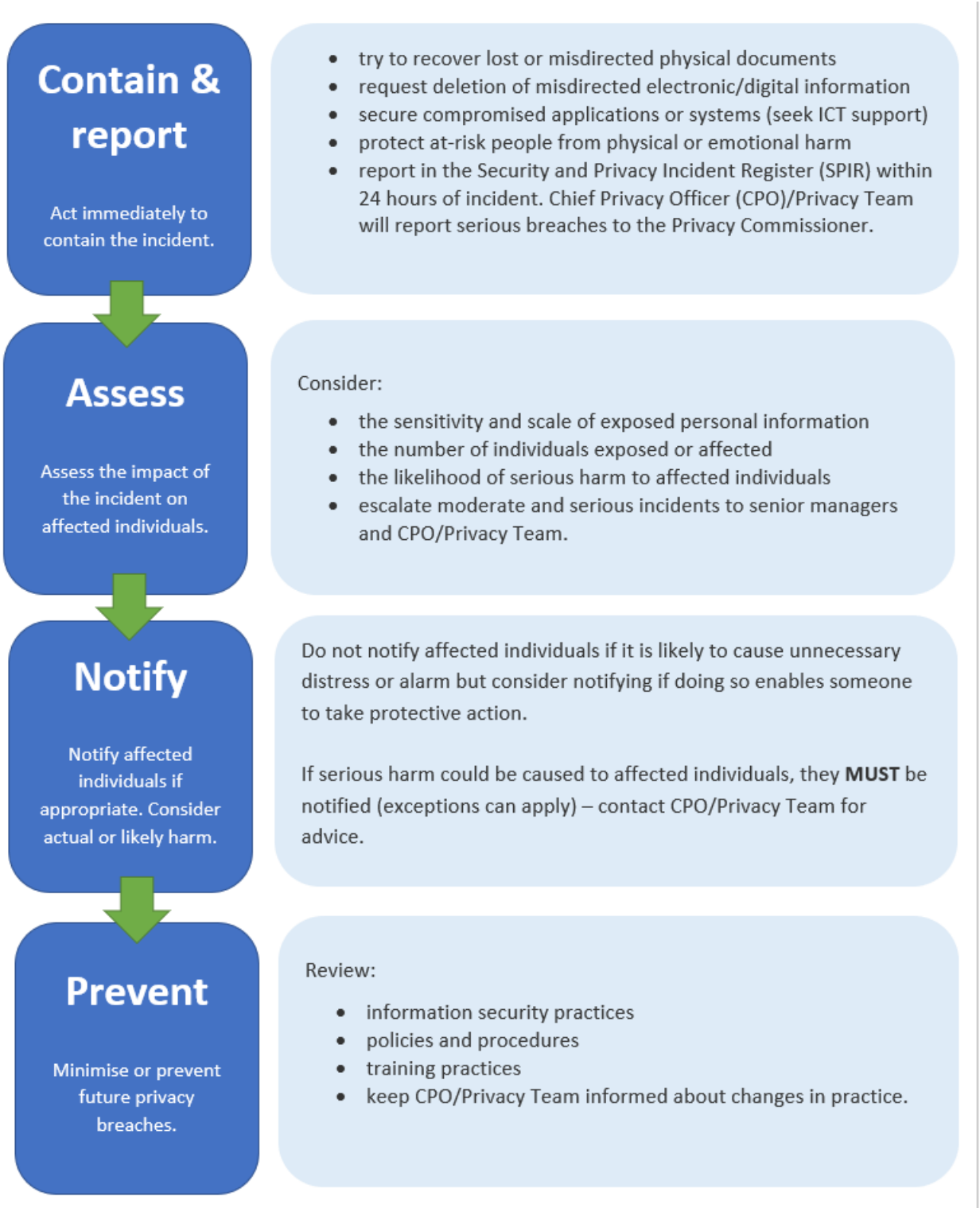
The Office of the Privacy Commissioner's website has helpful resources relating to information privacy, disclosure, information loss and privacy breaches.

Related Police Manual chapters

See these Police Manual chapters (or parts) for further information:

- 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

Privacy Breach: Response Steps (Quick guide)



Privacy Breach: Response Steps (Detailed steps)

Step	Description
1	Contain and report
2	Assess the impact
3	Notify (and apologise)
4	Prevent future breaches

Step 1: Contain and report

If you become aware of an actual, suspected, or potential privacy breach, take immediate steps to contain the breach and protect individuals against serious physical and emotional harm. At the same time, or soon afterwards, report the incident in SPIR (within 24 hours of becoming aware of the incident or issue).

Step	Action: Incident Responder/Reporter
1	Immediately contain the breach: - try to recover lost or misdirected physical documents - request and confirm deletion of misdirected electronic/digital information - shut down or secure compromised software or systems (contact Police ICT Service Desk for support) - stop the unauthorised practice - revoke or change computer access codes and/or remedy physical or electronic security weaknesses. Protect at-risk people from physical or emotional harm: - support temporary relocation of affected individuals and families if violence is indicated - refer or give advice to affected individuals about appropriate support services - provide advice about steps to mitigate or reduce the impacts of the breach incident.
2	Create a breach record in the Security and Privacy Incident Register (SPIR). The SPIR reporting tool will auto-populate your contact and position details and line manager. Complete the required fields, describe the incident and the actions taken to contain the incident. Relevant documents can be electronically added to the SPIR record. When you submit the SPIR report, an email notification is triggered to your line manager and your designated SPIR Manager (it will often be your District Operations Manager). Escalate moderate and serious incidents to your senior manager and CPO/Privacy Team Be available to assist in managing the incident and, if required, lead the early investigation and make initial recommendations.

Step 2: Assess the impact

To work out what immediate steps to take, consider the nature of the personal information involved, the context in which it has been compromised and the actual or possible impacts on affected individual/s. The following questions support decision-making about whether the incident meets the 'serious harm' threshold. Incidents meeting the threshold require formal notification to affected individuals and the Privacy Commissioner.

Step	Action: Incident Responder, SPIR Manager, District Ops Manager, CPO/Privacy Team

1

Information type and sensitivity

What is the nature of the compromised information?

Generally, the more sensitive the information, the higher the risk of serious harm to individuals. Victim, witness and informant information, criminal history, health, and financial information is considered inherently sensitive. However, physical address and contact information can also be highly sensitive information in the wrong hands.

The compromise of a combination of information like name, date of birth and address elevates the risk of serious harm, for example, it may enable someone to commit identity theft.

For example, a list of people spoken to by Police may not be sensitive in many cases, but it could be sensitive if witnesses have been given an assurance of confidentiality of their statements or involvement.

2

Context of information loss or disclosure

What is the context in which the personal information has been compromised?

The context in which information has been compromised is a key factor in determining the level or risk of harm and what immediate steps should be taken to protect affected individuals.

- Who has been affected? (e.g., a victim, witness, informant)
    - these classes of individuals are higher risk = elevates seriousness.
- How many people have been affected?
    - a greater number of people affected increases the privacy impact and risk of serious harm.
- Is the information in the possession of someone likely to cause harm or someone likely to be helpful?
    - Helpful person = low risk of serious harm, otherwise risk of serious harm is elevated.
- What is the nature of the potential harm? (e.g. physical safety, identity theft, financial loss, humiliation, reputational or relationship damage)
    - any identified risk to physical safety should be treated seriously
    - other types of harm can range from low impact to serious.
- Are there any security protections applied to the information? e.g., passwords, encryption
    - the stronger the security protection the lesser the risk of serious harm

The compromise of a combination of sensitive personal information, along with name, address and date of birth, puts affected individuals at a higher risk of serious harm.

3

Status of the breach

What has been done to recover or protect individuals from further harm?

- Is there a risk of further access, use or disclosure, including via social media or online?
    - information exposed on the internet is almost impossible to contain and can cause ongoing serious harm.
- If information was stolen, can it be determined whether the information was the target of the theft?
    - if the information loss was incidental to the theft, serious harm is less likely.
- Has the personal information been recovered?
    - if information has been returned or recovered the risk of future harm is diminished.
- Have effective steps already been taken to mitigate actual or potential harm?
    - effective and early action to contain an incident minimises harm to affected individuals.

4

Harm to Police

What harm to Police could result from the breach?

A privacy breach incident has the potential to cause serious reputational damage to Police, resulting in a loss of public trust and confidence. Examples include compromise of criminal investigation, loss of trust and confidence, reputational damage.

5	**Escalation decision making** (responder/SPIR Manager/Chief Privacy Officer) **Consider next steps to manage the incident** - Review the breach record and decide whether breach is minor and can be (or has been) effectively managed (SPIR Manager/CPO/Privacy Team) - you may identify incorrect risk assessment and/or opportunities. - Escalate moderate and serious incidents to your senior manager and CPO/Privacy Team - get support from managers and specialists to improve our incident response. - Does an Incident Management Team need to be assembled? (Senior manager/CPO/Privacy Team) - it may be appropriate to assemble a team to coordinate the response to a large-scale incident. If an Incident Management Team is to be assembled, include the Chief Privacy Officer and District Operations Manager and consider including the Chief Information Security Officer, Legal, HR, Integrity and Conduct, PNHQ Media (a communications plan may be required), and ICT representative (if subject matter expert is required).

Step 3: Notify (and apologise)

The decision to notify individuals about a breach incident is based on the impact assessment at Step 2.

Police must (with some exceptions) promptly notify individuals who have experienced, or are likely to experience, serious harm from a breach incident. Notifying individuals gives them a chance to take steps to prevent, limit or reduce further harm to themselves.

The Privacy Commissioner must also be notified where a breach is serious. The CPO/Privacy Team will do this once they are aware of the incident and have made their own assessment of harm.

Where Police actions have resulted in, or contributed to, the breach incident, take the opportunity to apologise to the affected individual.

To promote trust and confidence in Police, it can be beneficial to notify and apologise to individuals about less serious breach incidents, but care is needed to ensure any notification does not have the effect of causing unnecessary distress or alarm.

Step	Action: Incident Responder, SPIR Manager, District Ops Manager, Chief Privacy Officer/Privacy Team
1	**Deciding whether to notify** **Serious harm incidents** Based on the Step 2 assessment, Police must notify individuals who have been or are likely to experience serious harm from a breach incident (Privacy Act 2020, s.117). Notification of affected individuals can be delayed or bypassed if the circumstances match one of the exception criteria in the Privacy Act 2020 (s.116). Contact the CPO/Privacy Team for advice. **Notifying all other incidents** Police is under no legal obligation to notify individuals about incidents it considers do not raise issues of serious harm. However, it is good practice to tell people about an incident if it gives them the opportunity to take some action to avoid or lessen the impact of that incident. If notifying the individual may cause distress or alarm, particularly where the risks or impacts are low, it is better not to notify.

When, who and how

When to notify

Police are required to notify affected individuals 'as soon as practicable'. Do not wait until you have fully completed an investigation. You do not need to know exactly how an incident happened before notifying - the key is to notify serious incidents promptly. However, sometimes it may be necessary to delay notification to avoid compromising an investigation.

Who to notify

Police should notify individuals affected by serious breaches that it has caused. Police should also notify affected individuals of breaches involving third-party service providers that hold or process personal information on Police's behalf.

PNHQ's CPO/Privacy Team will notify serious incidents to the Office of the Privacy Commissioner. Alternatively, the Director: Assurance performs this task.

How to notify

- Where practicable, notify individuals on a one-to-one basis, either in person, by phone, email, or by letter from a senior officer serving the local community or region. Seek advice from the local SPIR Manager or contact the PNHQ CPO/Privacy Team.
- Where direct notification is impractical, notification can be made indirectly by public notice. For example, on Police's website, a news media website, a gazette notice, or via announcements on radio or television. Always discuss any proposed public notification beforehand with the CPO/Privacy Team. Public notification of a privacy breach requires Senior Manager approval, including Executive Director/Director, District Commander or higher roles.
- Using multiple channels to notify may be appropriate for a large-scale event - seek advice from the CPO/Privacy Team.
- Consider whether the method of notification might increase the risk of harm, for example, by alerting perpetrators via a public notification about the value of the compromised information.

What should be included in the notification?

The Privacy Act (s.117) prescribes what must be covered in the notification to an affected individual (or representative) and to the Privacy Commissioner.

- **To individuals,** Police must notify:
  - describe what has happened and the nature of the information at risk
  - tell them whether Police knows who has the information without identifying that person or agency (unless it is necessary to prevent or lessen a serious threat to the life or health of any person)
  - explain the steps Police has taken or will take to respond to the breach including what Police has done to control or reduce harm
  - advise the individual of steps they may wish to take to avoid or reduce harm on themselves and the nature of any assistance Police can provide
  - confirm that the Privacy Commissioner has been notified
  - advise them of their right to make a complaint to the Privacy Commissioner
  - provide the individual with a contact person in Police for further enquiries.

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

Guidance to assist individuals to protect themselves against identity theft can be found:
https://www.police.govt.nz/advice-services/cybercrime-and-internet
https://www.consumerprotection.govt.nz/general-help/scamwatch/
https://www.cert.govt.nz/individuals/
http://www.netsafe.org.nz/

- To the Privacy Commissioner, Police must notify:
  - the nature of the breach, including the number of affected individuals and the identity of the person or agency in possession of the information
  - the steps Police has taken or will take in response to the breach
  - whether affected individuals have been or will be contacted
  - if indirect notification is to occur, the rationale for doing so
  - the reason for any delay in notification
  - details of other agencies notified of the breach and why
  - a contact person within Police for further inquiries.

4

Others to contact

Independent Police Conduct Authority (IPCA)

If:

- a complaint against Police is received under s.15 Independent Police Conduct Authority Act 1988
- the matter involves criminal offending or serious misconduct by a Police employee and the matter is likely to place Police's reputation at risk (see Police/IPCA MOU).

Notify through the District or Service Centre Police Professional Conduct Manager (and where appropriate, notify the Authority).

See the Police investigations of complaints and notifiable incidents chapter for further information.

Consider if other internal or external parties need to be notified, including:

- Chief Information Security Officer, PNHQ
- Government Chief Privacy Officer at DIA
- National Cyber Security Centre (unauthorised/attempted access or use of computer systems)
- Third party contractors or other affected parties
- Media/communications
- Police Professional Conduct
- Police Association/Police Leaders' Guild
- Office of the Minister of Police.

Step 4: Prevent future breaches

Investigate root cause

Once initial response steps to contain, assess, and notify are completed, seek to identify the root cause of the incident if it is not already apparent. This could include a review of policies, procedures, training, or systems to reduce the risk of similar incidents occurring.
The level of investigative effort should reflect the significance of the breach, and whether it was a systemic breach or an isolated incident. Sometimes, system settings can be changed so that it is harder to make mistakes and to prevent human error.

Disciplinary steps

The objective of reporting privacy breach incidents is not about attributing blame and taking disciplinary action. Mistakes happen 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
- malicious or criminal actions, a Police investigation may be commenced.

Prevention plan

For significant breach incidents, a structured approach to prevention may be appropriate. A prevention plan may include:

- a security audit of physical and technical security
- a review of policies and procedures
- a review of training practices
- a review of third-party service provision.

A prevention plan may require an audit process to ensure all matters have been addressed.

Notifiable Privacy Breaches

The Chief Privacy Officer provides a summary of all notifiable privacy breach incidents as part of regular reporting to the Security and

Privacy Reference Group (SPRG), the governance group that has initial responsibility for oversight of security and privacy risks in the organisation.