Information privacy principles

descriptions and examples of breaches of the IPPs
Purpose ..................................................................................................................................................3
Background ........................................................................................................................................3
Definitions ...........................................................................................................................................4
Principle 1: Purpose of collection of personal information .................................................................5
Principle 2: Source of personal information .........................................................................................8
Principle 3: Collection of information from subject ...........................................................................12
Principle 4: Manner of collection of personal information ................................................................16
Principle 5: Storage and security of personal information .................................................................19
Principle 6: Access to personal information .........................................................................................22
Principle 7: Correction of personal information ..................................................................................26
Principle 8: Accuracy, etc., of personal information to be checked before use ..............................29
Principle 9: Agency not to keep personal information for longer than necessary .........................32
Principle 10: Limits on use of personal information ..........................................................................35
Principle 11: Limits on disclosure of personal information ..............................................................39
Principle 12: Unique identifiers .......................................................................................................44
Purpose

This document provides guidance on common risks that could expose your agency to privacy breaches. Looking at each of the Information Privacy Principles (IPPs), this document describes:

- risks that could expose your agency to privacy breaches
- what a breach of each IPP could look like
- consequences of breaching each IPP for individuals and for agencies
- controls that could mitigate risks and prevent future breaches

A scenario is also provided for each IPP to help illustrate how risks and breaches might play out in a given situation. These scenarios and examples are not intended to provide an exhaustive list of risks and breaches. You will need to consider these in light of your agency’s own risk profile and the personal information your agency holds.

The term ‘privacy breach’ is often equated with a failure to keep information secure or an inappropriate disclosure of personal information. The purpose of this guidance is to provide privacy officers with a tool to broaden the discussion on privacy risks and breaches within their agencies to cover all the IPPs, so that a wide range of privacy risks can be identified and mitigated, and future breaches avoided.

Background

All agencies holding personal information about individuals have to comply with the Privacy Act.

There are 12 Information Privacy Principles at the core of the Privacy Act. These IPPs set out how agencies are to:

- collect personal information (IPPs 1 to 4),
- store personal information (IPP 5),
- provide access to (IPP 6) and correct (IPP 7) personal information,
- use (IPPs 8 and 10) and disclose (IPP 11) personal information,
- only keep personal information for as long as necessary (IPP 9), and
- use unique identifiers (IPP 12).

A breach of any of the IPPs can have significant consequences for your agency even if there isn’t a complaint to the Privacy Commissioner or an interference with privacy (i.e. a breach which causes harm to an individual as set out in section 66 of the Privacy Act 1993). Whether or not an action (or omission) by your agency is deemed to be a breach of an IPP will depend on the circumstances of that particular case.

---

1 This guidance document forms part of a suite of privacy related guidance developed by the Government Chief Privacy Officer. Further guidance can be found on the Privacy Leadership Toolkit: https://psi.govt.nz/privacyleadership.
## Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Agency</strong></td>
<td>An individual or organisation that holds personal information.</td>
</tr>
<tr>
<td><strong>Breach (or privacy breach)</strong></td>
<td>Non-compliance with an Information Privacy Principle. An action does not have to result in harm to an individual (i.e. an interference with privacy) to be a breach. Breaches can affect one or many individuals.</td>
</tr>
<tr>
<td><strong>Consequence of a breach</strong></td>
<td>The outcome of a breach. This includes:</td>
</tr>
<tr>
<td></td>
<td>• Harm to an individual(s) – see definition below.</td>
</tr>
<tr>
<td></td>
<td>• Impact on the agency – these include, for example, loss of reputation and public trust and confidence, impact on operational service delivery, awarding of damages and costs, changes to systems and processes, loss of confidence by staff in carrying out their work.</td>
</tr>
<tr>
<td></td>
<td>• Wider impacts across government – for example, loss of public trust and confidence in government as a whole.</td>
</tr>
<tr>
<td><strong>Harm</strong></td>
<td>Loss, detriment, damage or injury to an individual (including adverse effect on rights, benefits, privileges, obligations or interests; or significant humiliation, loss of dignity, or injury to the feelings of that individual) resulting from a breach of an IPP.</td>
</tr>
<tr>
<td><strong>Interference with privacy</strong></td>
<td>Breach of an IPP + harm to an individual. The exception is where the Privacy Commissioner or the Human Rights Review Tribunal is of the opinion that there is no proper basis for a decision relating to a request for access to or correction of personal information. In that case the breach will be an interference with privacy without the need for any evidence of harm.</td>
</tr>
<tr>
<td><strong>Personal information</strong></td>
<td>Information about an identifiable individual.</td>
</tr>
</tbody>
</table>

---

In practice, the terminology defining breaches will differ between agencies. The purpose of this document is to provide guidance on what may constitute a breach, however defined in your agency’s terminology.
Principle 1: Purpose of collection of personal information

Only collect personal information you really need

Ask yourself:

- What is your agency trying to achieve by collecting personal information?
- What personal information does your agency need to collect to achieve this purpose?
### If your agency:
- collects personal information without being able to clearly articulate why and how it will be used
- collects more personal information than is necessary for the given purpose

### Then potential consequences are:
- more personal information is collected than is necessary, meaning the consequences of any breaches of the other IPPs may be exacerbated.
- additional personal information has to be managed/stored by your agency incurring unnecessary costs without having a purpose for collecting it in the first place.

### What could be done to reduce the risk?
- Have a clear understanding of the outcome you’re seeking and the purpose for which personal information will be collected.
- Clearly define what personal information is necessary for achieving the outcome/purpose, and how it will be used before the information is collected. Ensure employees understand, and are able to explain to customers, the purpose and need for the personal information being requested.
- Only collect personal information that is required in order to achieve the business requirement/objective.
- Design privacy controls into systems and processes involving collection of personal information and regularly review the effectiveness of existing systems, processes and controls including when any changes happen. Provide assurance to management that privacy has been designed into systems and processes, including when changes are introduced.
Scenario

An agency has decided to email a customer satisfaction survey to all customers who have dealt with the agency in the last three months. Currently, the personal information held for each customer includes their name and email address only. The survey asks for additional details to be provided by the customer, including residential address, marital status and date of birth.

Management has included this request for additional information as they feel it might be useful in the future, but they do not have a clear understanding of how it will be used.

The customer is not told why this information is being collected or how the agency intends to use it.

Potential breach of Principle 1

The agency has requested and may receive personal information without a clear purpose for its collection or knowledge of why it is needed.

Responding to the issue

- Make management aware of the potential breach.
- Clarify whether there is a clear purpose for the collection and if there is one, how the information will be used.
- If there is no current intended use for the information, any information received should be removed from the agency records or the customer contacted to confirm whether they are comfortable with the intended purpose of collection.
- It may be useful to involve communications staff to assist with any communications required.

What should be done to prevent this happening in the future?

- Develop and document why personal information is being collected, the purpose for which it will be used, and exactly what information is required to achieve that purpose (have a formal policy in place).
- Ensure that all employees know about the policy and how it applies to their work.
- Ensure that all employees know to check in with the privacy officer if they are thinking about new collections of personal information.
Principle 2: Source of personal information

Get information directly from the person wherever possible

Ask yourself:

- How does your agency intend to collect personal information?
- Can your agency collect this information directly from the individual?
- Do any of the exceptions\(^3\) apply?

\(^3\) See page 11.
If your agency:

- collects information from someone other than the individual (another agency, third party service provider, individual):
  - when it could have been collected directly from the individual,
  - without consent,
  - without the legal authority to do so
- uses information not collected directly from the individual which could be misleading or inaccurate

Then potential consequences are

- the accuracy of the information collected cannot be assumed or ensured.
- an individual who is not aware that their personal information is being collected will not be able to access and request correction of the information.
- decisions may be made based on inaccurate information or information collected illegally or without authority which, even if correct, could result in a legal challenge to those decisions.

What could be done to reduce the risk?

- Processes and systems should be designed with Principle 2 in mind; including approved means of collecting personal information directly from an individual.
- Communication/correspondence used to collect information should be reviewed by the privacy officer or your agency’s legal advisors to ensure the collection of personal information is from the individual directly, or in line with an exception to Principle 2.
- Explicitly consider how best to collect information, including whether any of the exceptions apply for all collections of personal information.
- Clear decision-making processes for staff should be put in place for using exceptions (for example, when collecting information from an individual isn’t possible).
Scenario

In the survey the agency sent to customers, further details are requested about the customer’s immediate family. Specifically, the agency has asked if any close family members might be interested in receiving the same services, and for the names, birth dates and contact details of those individuals.

Several customers responded with information about their friends and families. The agency did not request or ensure that those family members authorised the provision of their personal information. This information is not publicly available.

Breach of Principle 2

The agency has collected personal information about an individual from someone else without ensuring authorisation was provided by the individual concerned or that the collection met another of the exceptions under Principle 2.

Responding to the issue

- Make management aware of the issue. It is a breach of Principle 2 and will likely also be a breach of Principle 3. The information should not have been requested or collected in this manner.
- One option is to safely destroy the information. The agency may not think the collection would ‘prejudice the interest of the individual concerned’ but that individual may disagree and if they receive unwanted communications, complain to the Privacy Commissioner.
- Get the communications team to help contact the survey participants to apologise for making the request, to inform them that the information will not be used and deleted, and providing contact details for the family members to use should they wish.

What should be done to prevent this happening in the future?

- Ensure that all employees know to check in with the privacy officer if they are thinking about new collections of personal information.
- Future surveys or correspondence could include information on how to contact the agency to find out more for interested friends and family to use, rather than asking respondents to provide contact information for other people.
Exceptions to Principle 2:

The information:
- is 'publicly available information'. Check the definition of ‘publicly available’ in the Privacy Act.
- will not be used in a form in which the individual concerned is identified
- will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

The individual concerned has authorised collection from someone else.

Non-compliance would not prejudice the interests of the individual concerned.

Non-compliance is necessary:
- to avoid prejudice to the maintenance of the law by any public sector agency, which includes the prevention, detection, investigation, prosecution, and punishment of offences
- to enforce a law that imposes a pecuniary penalty, e.g. payment of a fine or penalty.
- to protect the public revenue.
- for the conduct of proceedings before a court or tribunal.

Compliance:
- would prejudice the purposes of collecting the information.
- is not reasonably practicable in the particular circumstances.

The Privacy Commissioner has authorised the collection of personal information under section 54.
Principle 3: Collection of information from subject

Be open with people about what’s going to be done with their information

Ask yourself:

- Does the individual concerned know and have you told them:
  - That their personal information is being collected?
  - Why their information is needed and how it will be used?
  - If information is being collected under a particular law (and if so, which one)?
  - If the information will be disclosed to anyone else, and if so who?
  - If they can choose to not give their personal information, and what will happen if they do not?
  - That they can access and request correction of their personal information?
  - How to contact your agency that has their information?
- Do any of the exceptions\(^4\) apply?

\(^4\) See page 15.
<table>
<thead>
<tr>
<th>If your agency:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Collects personal information directly from the individual without telling them:</td>
<td></td>
</tr>
<tr>
<td>• the purpose for which it is being collected,</td>
<td></td>
</tr>
<tr>
<td>• how the information will be used, or</td>
<td></td>
</tr>
<tr>
<td>• to whom it will be disclosed</td>
<td></td>
</tr>
<tr>
<td>Then potential consequences are:</td>
<td></td>
</tr>
<tr>
<td>• individuals do not know that information is collected about them and why it is being collected, meaning they cannot help ensure that the information is accurate, current, and not misleading.</td>
<td></td>
</tr>
<tr>
<td>• similarly, individuals will be unaware of the consequences of not providing information and may be impacted because of that.</td>
<td></td>
</tr>
<tr>
<td>• individuals will also be unaware of their ability to request access to their information, check its accuracy and request its correction if necessary.</td>
<td></td>
</tr>
<tr>
<td>• decisions made on the basis of poor quality information could cause harm to individuals.</td>
<td></td>
</tr>
<tr>
<td>• individuals may discover later that their information has been collected without their knowledge and could lose trust in your agency and make their complaint public.</td>
<td></td>
</tr>
<tr>
<td>What could be done to reduce the risk?</td>
<td></td>
</tr>
<tr>
<td>• Tell people clearly and simply what information is being collected, why, how it will be used and to whom it will be disclosed.</td>
<td></td>
</tr>
<tr>
<td>• Use the Office of the Privacy Commissioner’s “Priv-o-matic” tool to compose a privacy notice.⁵</td>
<td></td>
</tr>
<tr>
<td>• For plain English guidance on privacy notices follow the Web Usability Standard and guidance on the New Zealand Government Web Toolkit when publishing privacy notices online.⁶</td>
<td></td>
</tr>
<tr>
<td>• Build privacy notices into your systems, processes and forms.</td>
<td></td>
</tr>
<tr>
<td>• Provide staff training in the collection and handling of personal information and ensure process guidance is clear and up-to-date.</td>
<td></td>
</tr>
</tbody>
</table>

Scenario

When the survey was sent to the respondents, it set out why the information was being collected and how it would be used. However, the survey did not let respondents know that their completed responses would be shared with a third party in order to offer the respondents further services. The respondents are surprised when they are contacted by the third party organisation.

Breach of Principle 3

The agency has not informed the individuals concerned of all intended recipients and uses of the information, nor that another organisation will hold the information as well as the agency collecting it.

Responding to the issue

In this scenario, it would have been reasonably practicable to inform the survey respondents of all intended recipients and uses, so:

- The agency should contact respondents with the additional information about the intended recipients and use of the information, and offering the option of opting out of the information being disclosed to the third party.
- The agency should also check whether the collection, use and disclosure of the information meet Principles 1, 10 and 11.

What should be done to prevent this happening in the future?

- Ensure that all employees know to check in with the privacy officer if they are thinking about new collections of personal information.
- Consider making disclosure to and use of the information by a third party an opt-in process for individuals.
Exceptions to Principle 3

These are similar to those in Principle 2.

Non-compliance can be authorised by the individual.

(Authorisation generally requires a positive action or decision by an individual, and they have to understand reasonably clearly what they are agreeing to.)

Non-compliance would not prejudice the interests of the individual.

(The agency may not think the collection would ‘prejudice the interest of the individual concerned’ but that individual may disagree and if they receive unwanted communications, complain to the Privacy Commissioner.)

Non-compliance is necessary for the same reasons as in Principle 2.

The information:
- will not be used in a form in which the individual concerned is identified
- will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

Compliance:
- would prejudice the purposes of collecting the information.
- is not reasonably practicable in the particular circumstances.
Principle 4: Manner of collection of personal information

Be fair about how you get it

Ask yourself:

- Was any reliance placed on an unlawful action to help collect information (such as keeping a recording of a phone call you were not a party to)?
- Was threatening or coercive behaviour used to collect information?
- Was the individual misled when collecting information?
- Would you feel comfortable telling someone how the information was obtained?
- Was the information sensitive?
- Was information collected at a place or time when the individual would have a stronger expectation of privacy?
- Was information collected in a covert manner when the individual might reasonably expect to be told of the collection?
**If your agency:**
- collects personal information unlawfully
- collects personal information unfairly
- collects personal information intrusively

**Then potential consequences are:**
- an individual may experience stress or other forms of emotional harm if pressured to provide personal information that is embarrassing or that they feel is excessive in the circumstances.
- an individual may feel forced to provide information when they do not have to.
- if the information is collected unlawfully, any decisions based on it are likely to be successfully challenged.

**What could be done to reduce the risk?**
- Make sure that when staff members collect personal information they understand to do so with respect and within the limits your agency has set on collection.
- Provide practical training to help staff deal respectfully with difficult, troubled, or emotionally upset customers.
- Put processes in place for review and quality assurance of communications with customers to ensure they are treated with respect.
- Develop and implement processes for dealing with complaints and make sure that customers can easily file complaints and receive progress reports.
Scenario

Five survey recipients did not provide details of family members when responding to the survey. An employee noticed that the services being provided for three of these respondents are still in progress. In an effort to obtain the family members’ details, the employee informed the respondents that until they provide the details their services will not be completed. Although not happy with the situation, the three respondents provided the requested information.

Potential breach of Principle 4

The agency, through the actions of its employee, has used unfair, manipulative and potentially threatening actions in an attempt to collect personal information.

Responding to the issue

- Make management aware of the issue. It is a breach of Principle 4.
- The information should not have been requested or collected in this manner.
- Get the communications team to help contact the survey participants to apologise for making the request in this manner, to inform them that the information will not be used and deleted, and to confirm continuation of services.
- Consider safely destroying the information collected under duress. The agency may not think the collection would ‘prejudice the interest of the individual concerned’ but that individual may disagree and if they receive unwanted communications, complain to the Privacy Commissioner.
- The employee’s manager should discuss the employee’s approach with them, and if necessary escalate the issue for appropriate resolution.

What should be done to prevent this happening in the future?

- Provide staff training in the collection and handling of personal information and ensure process guidance is clear and up-to-date.
- Put in place quality assurance processes for communications with customers to ensure they meet requirements under the Privacy Act and treat people with respect.
Principle 5: Storage and security of personal information

Keep it secure

Ask yourself:

- Is information protected by reasonable safeguards? e.g.
  - policies and procedures are followed by staff
  - access to physical documents is appropriately restricted
  - access to physical records’ storage is monitored
  - electronic documents or equipment are password protected and/or encrypted
  - information is protected from accidental and unauthorised modification.
  - information is only disposed of securely.
- Is information susceptible to loss? e.g.
  - is electronic information required to be transferred securely?
  - are backups performed regularly and kept securely?
  - is physical information handled carefully?
- Are policies and procedures clear as to storage and access to personal information?
If your agency:

- has inadequate identification and access management controls for personal information (whether for customers or employees)
- provides personal information to a third party that does not keep that information secure
- does not properly secure personal information (hard copy or electronic) when a staff member takes it away from agency premises (e.g. on their mobile device)
- disposes of personal information without using secure methods and processes
- exposes personal information to visitors who can see paper files on desks or on staff computer screens

Then potential consequences are:

- by not maintaining appropriate control of the information, then you risk breaching other Principles. For example, unauthorised external persons may be able to gain access to the personal information which could lead to physical, emotional or financial harm to an individual.
- employees may be able to browse information on other employees or individuals they know without an appropriate purpose for doing so.
- depending on the sensitivity of the information, other agencies may need to be involved, and the public may need to be informed. This could lead to a loss of public trust in your agency as well as in the rest of government.
- it can be both time and resource expensive to respond to a significant security breach.
- responding to a breach can severely disrupt an agency’s business (for example putting in place immediate controls such as shutting down systems or reactively putting in place new processes and procedures).

What could be done to reduce the risk?

- Put in place clear, easy to follow policies and procedures, supported by training and awareness raising.
- Check what security requirements apply to your agency. Public service departments and selected other agencies are required to meet certain standards for security of information, personnel, and other assets. These are detailed in the Protective Security Requirements, which include the New Zealand Information Security Manual (NZISM).
- Put secure processes in place for handling personal information when it has to be sent outside your agency or taken to another location.
- Ensure disaster recovery procedures for electronic information are in place and are regularly tested (regular backups, off-site backups etc.)
- Ensure information, whether physical or digital, is kept securely (password/combinations etc.).
- Ensure access to personal information is limited to employees with a demonstrable need and that digital footprints are tracked and audits conducted.
- Ensure software is kept regularly updated to ensure that known vulnerabilities are addressed promptly.
- Ensure mobile devices that may contain personal or confidential information are properly secured.
Scenario

In order to receive the survey responses, the agency had set up a temporary email account. The person who was supposed to monitor the mailbox and deal with the responses had an accident. Rather than asking IT to provide access to the mailbox, one of the injured person’s team mates, looked for and found the password to the temporary mailbox in her injured colleague’s drawer. That person then started responding to the emails.

Breach of Principle 5

The person who found the password was well intentioned but should have gone through the formal processes for getting access to the mailbox. By using the injured co-worker’s password, they have circumvented processes to provide control and auditability over personal information. If they were not entitled to view the responses, that could also be a breach.

While this is a breach of Principle 5, it may not have caused harm to the individuals whose information was used so would not necessarily be an interference with privacy.

Responding to the issue

- The helpful teammate’s manager should speak to them about the inappropriateness of using someone else’s password.
- Get the teammate formal auditable access to the mailbox if permitting that access is appropriate.

What should be done to prevent this happening in the future?

- Ensure all staff know that using another person’s password is unacceptable.
- Have backups organised to provide access to temporary mailboxes so that if the primary mailbox ‘owner’ is unavailable, the business activity can continue without undue delay.
Principle 6: Access to personal information

Let the person see it if they want to

Ask yourself:

- Does your agency have processes in place and people assigned to respond to requests for:
  - confirmation that your agency holds, or does not hold, information about the person making a request;
  - access to the personal information of the person who has made a request; and
  - doing so within the required timeframes?

- Is your agency able to confirm they have responded to personal information access requests with all relevant information?
  - Are individuals advised of their right to correct any incorrect information?

- Are there good reasons for refusing to give access to personal information, and if so is this clearly explained to individuals?
If your agency:

- does not provide access to personal information about the individual
- is not able to easily access personal information when requested
- does not respond to access requests within the statutory timeframes

Then potential consequences are:

- individuals have a legal right to confirmation of whether or not a public sector agency holds information about them and access to that information. This right can be enforced in a court of law.
- an individual who is refused access to their own information may not be able to protect themselves and their interests (for example, not knowing the information on which a decision affecting them was based, or not being able to check the accuracy of information to avoid consequences of identity theft).

What could be done to reduce the risk?

- Put in place a process for responding to access requests, including considerations of timeframes. Templates for responses can also be useful.
- Track and log access requests in order to provide assurance of compliance to management. Section 30 of the Privacy Act requires agencies to provide access unless your agency can justify refusal under sections 27-29.
- Create and make available a guide to the withholding grounds and how they may apply to the specific information your agency holds. Staff responding to requests should have this type of tool as a reference.
- A comprehensive and well-understood information management strategy that covers all areas and functions can help your agency to manage personal information in a way that makes it easier to respond to access requests.
- A personal information inventory could help you know what personal information your agency holds, its classification and how to access it when responding to access requests.

---

9 See Part 5 Section 40 of the Privacy Act 1993.
**Scenario**

The distribution of the survey has made several recipients curious as to exactly how much information the agency already holds about them. They have variously contacted the agency by phone, email, and one or two hard copy letters. A staff member has refused to accept the requests made by phone unless callers make their request in writing. They have done this without providing any explanation as to why they are making that requirement.

**Potential breach of Principle 6**

The agency is entitled and required to satisfy itself that the requestor is the individual the information is about or authorised by that person. This should have been explained to those phone callers and that the request for a written request in this case is to provide that assurance.

**Responding to the issue**

- The agency should ensure that all callers receive a follow-up call to explain why they were asked to provide a written request and offer assistance with completing their request as required by s.38.
- The agency could offer various options for verifying identity and giving access to the information (for example, the requestor could come to the office in person with a form of identification).

**What should be done to prevent this happening in the future?**

- Ensure that agency staff members who answer phone calls are aware of the requirements to assist people wishing to have access to their personal information.
- Update the process document for responding to personal information with appropriate guidance on how to handle requests over the phone.
- Ensure policies and procedures are in place for assessing the level of identity verification needed in line with the sensitivity of the information.
Good reasons for withholding

The reasons for which agencies can refuse access to personal information about an individual are set out in sections 27-29 of the Privacy Act. How Principle 6 interacts with other enactments and Acts of Parliament is set out in section 7(1)-(3).

Some of the most common reasons for refusing access include the following:

- The information is evaluative material as defined in section 29(3) and disclosure would breach an express or implied promise of confidentiality made to the person who supplied it
- Giving access to the information would disclose the personal information of another individual
- The information is not readily retrievable.
Principle 7: Correction of personal information

Fix it if the person thinks it’s wrong

**Ask yourself:**

- If an individual requests that their information be updated, and provides updated information, do processes exist to ensure that this occurs?
- Even if you do not think a correction is justified, do processes exist to ensure that a note recording that the individual has asked for a correction and the details of that, is documented on their file?
- Does your agency allow individuals to correct their personal information through an online account?
- Does your agency inform individuals that they can provide their own statements of correction if necessary?
- Are corrections and statements of correction sent to other parties who may have received information from your agency?
### If your agency:

- Holds information about an individual that is not accurate
- doesn’t meet its legal obligation to either correct an individual’s personal information or attach a notice of correction to the file

### Then potential consequences are:

- if not corrected, incorrect information that is considered by your agency (or other agencies) to be an authoritative data source could harm an individual through refusal / loss of benefits and services.
- if not corrected or flagged as being disputed (through a statement that correction was sought), your agency could rely on wrong or disputed information to make decisions which may leave them open to being successfully challenged.
- Information left uncorrected (e.g. address) can lead to further breaches, for example disclosure of personal information to someone other than the individual concerned.

### What could be done to reduce the risk?

- Put in place a process for responding to correction requests, including considerations of timeframes and, potentially, templates for responses.
- Create and make available a guide for staff responding to correction requests.
- Correction requests that are received, but which your agency decides not to action because the facts are under dispute or for some reason, should be documented on the individual’s record. You should notify the individual, and the notification should state that the individual may provide a statement of correction if they are not happy with your agency’s notation.
- Log correction requests and document the decision process followed in order to assure management of your agency’s compliance. Many systems offer logging and audit trail capabilities which may assist in tracking changes made to the information.
- You may need to provide training to staff in how to respond to access and correction requests.
- Consider providing individuals with online or phone access that enables them to update their own data. Such access mechanisms will need reasonable processes and security to ensure the individuals concerned are the ones editing the information and not an unauthorised third party. You may want to consider whether some information is not appropriate for editing in this way because it relates to verified identity information.
Scenario

After the survey, a respondent contacted the survey team at the agency to correct all their personal information. The survey team staff who process responses do not update the contact management system with these details because there is a ‘proper procedure’ for people to use to notify the agency about changes to personal information. The request is not passed on to relevant staff and a statement of correction isn’t added to the respondent’s file.

Breach of Principle 7

The personal information held about this respondent was not updated after they provided correct information to the agency, and a notice that correction was sought has not been attached to the information.

As a result of this breach of Principle 7 there is also a probability of breaching Principle 8: personal information that is no longer accurate continues to be used even after the individual has provided corrected information and the individual may not receive appropriate services from the agency.

Responding to the issue

- The agency has an obligation to check the accuracy of personal information before using it. Correction of information would normally be done through a designated process to ensure its accuracy. Since the updated email address wasn’t received through the designated process, the administrator could contact the respondent to check, or attach note that correction was sought to the respondent’s file.
- In practice there is little that can be done immediately to respond to this issue as it may not be discovered until something goes wrong, e.g. the individual does not receive important services.

What should be done to prevent this happening in the future?

- See the section on What could be done to reduce the risk?
- Raise the awareness of staff of individuals’ rights to access and correction of their information.
- Also, any correspondence with customers should tell them that they can request to have their information corrected and how to do so.
- Put a process in place for identifying updates to personal information received outside normal processes and verifying them before the information is used.
Principle 8: Accuracy, etc., of personal information to be checked before use

Take care that it’s accurate before using it

Ask yourself:

- How often is accuracy of personal information confirmed?
- How frequently is that personal information used?
- How is the accuracy of personal information validated?
- Is data collected in bulk or indirectly from another agency subjected to the same level of accuracy confirmation?
- Does your agency obtain information indirectly without the individual’s knowledge or consent? If so why?
If your agency:

- uses personal information that is not:
  - accurate
  - up to date
  - complete, or
  - relevant
- uses personal information that is misleading

Then potential consequences are:

- inaccurate data may result in different decisions from those based on accurate information; this could lead to harm for the individual (such as not receiving an entitlement).
- wrong contact details could lead to delays in providing services to a client and could also lead to disclosing their personal information to someone else.

What could be done to reduce the risk?

- Put processes in place to help ensure the information your agency collects and holds about people is accurate and current.
- Collect information directly from the individual unless an exception applies. Information collected directly from an individual is often more likely to be accurate.
- When you collect information from the individual, you can put processes in place for them to review the data for accuracy.
- When conducting business with individuals, routinely ask them to verify that their information is current. This will help maintain the information’s accuracy.
- Other checks you could carry out include checking the data against another reliable source, or recording the date and source of the information so that your agency can say how, when and where the information was obtained if the information is questioned.
- Agencies could put systems and processes in place to identify personal information that is subject to change and that periodically remind or require employees to confirm the accuracy of the information before use.
Scenario

The agency sends out letters thanking respondents for their participation in the survey. One of the letters is sent to the wrong address. The address details had been updated by the respondent but this had only been actioned in the agency’s contact management system and not replicated to the survey database.

The uncorrected details were the respondent’s former address and name prior to a separation from their partner. The ex-partner is still living at the old address.

Breach of Principle 8

Use of inaccurate contact details, of which the agency should have been aware, has resulted in the customer’s former partner becoming aware that their ex-partner has dealings with the agency.

Inaccurate personal information has been used, although the agency had the ability to check this against information held elsewhere.

Responding to the issue

- The breach of Principle 8 in this scenario has also led to a potential disclosure of personal information to someone other than then customer concerned (a potential breach of Principle 11).
- The agency should have internal processes for responding to breaches. Those should be informed by the Privacy Commissioner’s Voluntary Breach Guidelines. (https://www.privacy.org.nz/news-and-publications/guidance-resources/privacy-breach-guidelines-2/) See also the section on Principle 11.
- In this scenario, the agency should contact the customer and apologise and determine any harm that needs to be mitigated.

What should be done to prevent this happening in the future?

- The agency should put processes in place to ensure that information updated in one of their data stores is also updated across all their data.10
- See the section on What could be done to reduce the risk?

---

10 In some cases, individuals may have chosen to have different information recorded in different places. If your agency has reason to believe that an individual has chosen to have different information recorded, this should be taken into account when updating data across multiple data stores.
Principle 9: Agency not to keep personal information for longer than necessary

Dispose of it when it’s no longer needed

Ask yourself:

- Has your agency determined how long it needs to keep the information to achieve the purposes for which it was collected?
- Has your agency also determined what other lawful purposes the information may be used for and how long it needs to be kept for those purposes?
- Does your agency have an approved Disposal Authority from Archives New Zealand?
- Does your agency have processes in place to implement the Disposal Authority or the General Disposal Authorities issued by Archives New Zealand?\(^{11}\)
- If the information is to be destroyed, do your processes ensure:
  - Personal information is de-identified where appropriate?
  - Shredders and/or secure destruction services are used?
  - Hard drives of computers, photocopiers, phones, etc. are securely erased before sale or decommission?
- Back-up files, as well as originals, are deleted?

---

### If your agency:

- keeps personal information for longer than is needed to achieve the purpose of collection and any other lawful purposes for which the information can be used
- keeps personal information longer than needed, and in that time the information’s accuracy and currency become questionable
- uses personal information just because it is available (function creep) and the information wasn’t collected for that purpose and the purpose isn’t otherwise a lawful purpose

### Then potential consequences are:

- once the purpose for collecting personal information is no longer relevant, retaining this information means that using it could also breach Principles 1 and 10.
- your agency incurs costs to store and manage information for which it has no use.
- personal information that your agency no longer actively uses is less likely to be managed or stored securely which then risks breaching Principle 5 and possibly Principle 11.
- information that is not in active use has a higher risk of becoming inaccurate, out of date and misleading leading to a breach of Principle 8.

### What could be done to reduce the risk?

- Ensure you have a Disposal Authority in place and implement procedures to ensure that all public records (including personal information) are disposed of in accordance with a General Disposal Authority or an agency-specific Disposal Authority.
- Design systems and processes to record a date of expiry or review (of whether it should be disposed) for personal information that aligns with the business need for it. Many systems have the functionality to apply these dates from the point of collection.
- Put in place an internal policy that:
  - details the requirements for ensuring all personal information is disposed of in a secure and appropriate manner, and
  - ensures systems/processes are in place to monitor and report compliance with the policy.
Scenario

The information obtained during the survey is collated and a marketing strategy developed based on the responses. Once the information has been processed, the agency’s management team does not dispose of the response records. This includes responses from people who ticked the box that said “I do not want to be contacted about my responses to the survey”. The responses are no longer needed for the purpose for which they were collected and there isn’t another lawful purpose for which they can be used. The agency does not have policies or processes in place to guide employees on proper disposal of information, so staff members usually keep personal information ‘just in case’.

Breach of Principle 9

The agency has not met its responsibility to properly manage the retention and disposal of personal information.

Responding to the issue

- At this stage the retention of the information may not mean that there is an ‘interference with privacy’ because there is no indication yet that keeping the information has caused harm.
- However, if someone in the agency uses the information to contact a survey respondent who has requested not to be contacted, that would be a breach of Principle 10 and the person may complain to the Privacy Commissioner.
- Assess the information and make considered decisions about what information should and should not be kept and make safe arrangements for disposal of information that will not be kept.

What should be done to prevent this happening in the future?

- The agency should put policies and processes in place to ensure that personal information is properly managed throughout its useful life and disposed of safely when it is no longer useful for the purpose for which it was collected or another lawful purpose.
- Those purposes include providing access to individuals who wish to know what information the agency holds about them or who request that information about them is corrected or updated.
- Managers and staff should be trained in proper recordkeeping practices and the importance of following them.
Principle 10: Limits on use of personal information

Use it only for the purpose you got it

Ask yourself:

- What business purpose(s) was the information collected for? Is the information being used for any other purpose(s)?
- Does your agency have any statutory authority to collect and use information and are there any restrictions on that?
- Does your agency have a clear understanding of “directly related” purpose,\(^\text{12}\) and is it robustly communicated to staff?
- Are staff trained in the acceptable use(s) of personal information to which they have access?
- Is misuse of personal information a breach of your agency’s Code of Conduct? What are the penalties for such a breach?
- Do any of the exceptions\(^\text{13}\) provided by the Privacy Act apply?
- Are the purposes in connection with which unsolicited information is received recorded?

\(^{12}\) As per exception (e) – “That the purpose for which the information is used is directly related to the purpose in connection with which the information was obtained”

\(^{13}\) See page 38.
### If your agency:

- uses personal information obtained in connection with a specific purpose for another, non-directly related purpose
- has unclear or no limits or controls over the use of personal information by people within your agency

### Then potential consequences are:

- information collected for an unrelated purpose is used in making a decision about an individual that disadvantages them because the information used is insufficient or misleading for the new purpose.
- information collected for one purpose is combined with information collected for an unrelated purpose and the apparent contradictions or inconsistencies adversely affect how the individual is treated.
- staff use information obtained for an unrelated purpose and draw inferences that are in error because the information is incomplete for the new purpose.
- individuals receive unsolicited interaction with your agency resulting in loss of trust and confidence in your agency, and which could also adversely affect them.
- individuals believe their personal information has been used without permission or contrary to the purpose for which it was collected.

### What could be done to reduce the risk?

- Put in place a clear policy around what personal information it holds and what the information may be used for.
- Provide training to staff members on the proper use and handling of personal information and ensure that process guidance is clear and up-to-date.
- Put in place quality assurance processes for communication with customers.
- Communications/correspondence/forms etc. used to collect information should be reviewed to ensure that they clearly communicate the purpose(s) for the information collection and that the stated purpose(s) aligns with the intended use(s) of the information.
- Design and build your systems and processes to only allow access and use of personal information for the purposes defined in your agency’s policy (See Principle 1).
Scenario

When the survey was sent to the respondents, it set out why the information was being collected and how it would be used. After receiving the responses, the agency realised it could use the information to offer new services to the respondents through sharing the information with a third party. The respondents are not aware of this additional purpose until they are contacted by the third party. Several respondents complain to the agency about how their information has been used.

Breach of Principle 10

The agency has used the information it collected from respondents for a different purpose to the purpose in connection with which it was collected. The agency had not told people the information would be used in this way, meaning that the respondents were not aware and did not authorise this use of their information.

Responding to the issue

- The agency should check its records to determine whether the use of the information by a third party to offer new services was considered to be a directly related purpose prior to sending the information to the third party.
- The agency should treat this case as breaching Principle 10 and compose a letter of apology to all the individuals who had been contacted by the third party and offered further services. The individuals could be provided with a process for opting into receiving offers of further services should they want.
- The personal information should be retrieved from the third party.

What should be done to prevent this happening in the future?

- Put in place policies and business processes for determining the ways in which personal information collected through surveys can be used.
- Develop guidance on how to deal with this scenario in the future and make staff aware of the issue.
- Think about what potential uses are likely to be and take these into account when designing surveys in the future and when informing people of how the information will be used.
- Ideally give participants choice whether or not they are willing to be contacted for further information. This should be in the form of an opt-in mechanism or process that can be recorded against their information.
- Put policies and processes in place to ensure that personal information collected through surveys is properly used throughout its useful life.
Exceptions

- An agency that holds personal information that was obtained in connection with one purpose shall not use the information for any other purpose unless the agency believes, on reasonable grounds,—
  a) That the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to use the information; or
  b) That the use of the information for that other purpose is authorised by the individual concerned; or
  c) That non-compliance is necessary—
     i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or
     ii) For the enforcement of a law imposing a pecuniary penalty; or
     iii) For the protection of the public revenue; or
     iv) For the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
  d) That the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to—
     i) Public health or public safety; or
     ii) The life or health of the individual concerned or another individual; or
  e) That the purpose for which the information is used is directly related to the purpose in connection with which the information was obtained; or
  f) That the information—
     i) Is used in a form in which the individual concerned is not identified; or
     ii) Is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
  g) That the use of the information is in accordance with an authority granted under section 54 of the Privacy Act 1993.
  h) That the information—
     i) Is used in a form in which the individual concerned is not identified; or
     ii) Is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
  i) That the use of the information is in accordance with an authority granted under section 54 of the Privacy Act 1993.

---

14 Note that an amendment was passed on 30 June 2015 to the ‘publicly available’ exceptions to Principles 10 & 11.
Principle 11: Limits on disclosure of personal information

Only disclose it if you have a good reason

Ask yourself:

- Why is the personal information being disclosed?
- Does your agency have authority to disclose the information?
- Do any of the exceptions\(^\text{15}\) apply?
- Is there an approved process for disclosing personal information and is it well understood?
- What protections are in place for personal information disclosed to third parties including contractual terms and assurance processes over transfers, security, handling, and disposal?
- Where information is required to be disclosed, are the processes robust and do they ensure that only the information that should be disclosed is disclosed?
- Are records kept of all disclosures, including the reasons for disclosure, recipient, methods of transfer, security protocols, and other relevant provenance type information?
- If disclosing (or publishing) aggregate or de-identified data, has your agency ensured that individuals can’t be re-identified?

\(^{15}\) See page 43.
<table>
<thead>
<tr>
<th>If your agency:</th>
<th>Then potential consequences are:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• allows unauthorised persons to access personal information (whether of customers or employees) because of inadequate and access management controls</td>
<td>• unauthorised persons (including employees) may be able to access the personal information of the individual; this can result in physical, emotional or financial harm to the individual.</td>
</tr>
<tr>
<td>• inappropriately discloses personal information to another individual or agency (public/private/non-governmental) by</td>
<td>• if the disclosure is the result of a security or access/authentication weakness, then both Principles 5 and 10 may be breached.</td>
</tr>
<tr>
<td>o by disclosing personal information without being authorised by the individual or without your agency having some statutory or other authority to do so</td>
<td>• the disclosure becomes publicly known or your agency may need/want to report it to the Privacy Commissioner. This could cause a loss of public trust in your agency as well as in the rest of government.</td>
</tr>
<tr>
<td>o not appropriately managing spreadsheets that contain personal information for reporting or other purposes</td>
<td>• it can be both time and resource expensive to respond to a significant disclosure breach.</td>
</tr>
<tr>
<td>• de-identifying data without understanding appropriate methods of de-identification leading to:</td>
<td>• responding to a disclosure breach can severely disrupt your agency’s business, for example, putting in place immediate controls such as shutting down systems or reactively putting in place new processes and procedures.</td>
</tr>
<tr>
<td>o anonymised or aggregate data still being able to be used to identify an individual; or</td>
<td>• reputational damage may cause customers to provide inaccurate or incomplete information in the future or refrain from using services to which they are entitled.</td>
</tr>
<tr>
<td>o individuals actually being identified despite efforts to anonymise data?</td>
<td>(Note: Agencies cannot ‘contract-out’ the accountability for complying with the Privacy Act to third parties such as service providers. It is your agency’s responsibility to ensure that the third party has adequate processes in place. Poor practice by third parties can reflect badly on you.)</td>
</tr>
</tbody>
</table>
## What could be done to reduce the risk?

- Put in place policies, procedures and guidance in place to manage disclosures of personal information. Compliance with them should be monitored and reported to senior management.
- Design systems and processes to:
  - identify documents and systems containing personal information;
  - manage access to the information held in those documents and systems; and
  - log and report on all access to personal information including look-ups.
- Periodically review what data is disclosed internally and to other agencies to ensure that the disclosures are still warranted and that the processes are still robust and that security is adequate.
- Assess the distribution and publication of analysis, research, and data collation that involves personal information to ensure that individuals are adequately protected and not inadvertently identified or identifiable.
- Put in place mechanism for gaining assurance over a third party’s systems, policies and processes. It is your agency’s responsibility to ensure that a third party has adequate processes in place for dealing with personal information. Agencies cannot, ‘contract out’ the accountability for their compliance with the Privacy Act.
- Regularly review the risks of using third parties (including consideration of the types/sensitivities and quantities of personal information involved) and develop assurance plans to respond to those risks.
- Ensure there is regular reporting to management on the results of assurance activities.
Scenario

Another agency is impressed with the results of the survey as reported in the agency’s Annual Report. The second agency decides they should do something similar and ask for the survey to be sent to them so they can re-use it.

An employee of the first agency sends the second agency a copy of the survey questions. Unfortunately, the document sent contains the answers from a respondent, including identifying details, because the document was incorrectly filed.

Breach of Principle 11

The agency has provided personal information to another agency without authorisation.

Fortunately, the employee of the second agency who received the file and opened it saw the error and immediately deleted it from their inbox and their electronic ‘trash/recycle’ bin. They notified their service desk to remove all copies of it from their servers. They called the employee of the first agency to notify them and to request a copy of the survey without any answers in it.

Responding to the issue

- Because of the knowledgeable response by the employee at the second agency, there has been a very limited disclosure of the respondent’s answers to the survey.
- The employee of the first agency should follow their agency’s procedures for analysing the cause of the breach and follow through on mitigating actions so that this mistake does not happen in the future.

What should be done to prevent this happening in the future?

- The employee of the first agency should have double-checked the file before emailing it - because people make mistakes and documents get misfiled and are given uninformative or misleading file names.
- The first agency’s email system could be set-up to intercept emails with file attachments and query the sender to double-check what they are sending.
- The survey proper and the respondents’ return should be filed in separate subsections of the document/records management system to minimise the risk of such mistakes happening.
- The agency should put policies and processes in place to ensure that personal information collected through surveys is properly used throughout its useful life.
Exceptions:

Unless the agency believes, on reasonable grounds –

a) That the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or

b) That the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to disclose the information; or

c) That the disclosure is to the individual concerned; or

d) That the disclosure is authorised by the individual concerned; or

e) That non-compliance is necessary –
   (i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, investigation, prosecution, and punishment of offences; or
   (ii) For the enforcement of the law imposing a pecuniary penalty; or
   (iii) For the protection of the public revenue; or
   (iv) For the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

f) That the disclosure of the information is necessary to prevent or lessen a serious and imminent threat to-
   (i) Public health or public safety; or
   (ii) The life or health of the individual concerned or another individual; or

h) That the information –
   (i) Is to be used in a form in which the individual concerned is not identified; or
   (ii) Is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

i) That the disclosure of the information is in accordance with an authority granted under section 54 of this Act.
Principle 12: Unique identifiers

Only use “unique identifiers” where it’s clearly allowed

Unique identifiers are: something that is assigned to an individual by an agency for the purposes of the operations of the agency and that uniquely identifies that individual in relation to that agency. The individual’s name is not a unique identifier for the purpose of the Privacy Act.

Ask yourself:

- How is a person identified in your agency’s systems?
- Have you assigned a unique identifier to each individual to be used in the operation of your agency’s systems and processes?
- Is the unique identifier necessary for your agency to carry out its functions efficiently?
- Are you re-using another agency’s unique identifier without authority?
- Do you know if there is a Code of Practice that regulates the use of the unique identifier?
- Are you using a unique identifier, or a shared unique identifier in accordance with applicable Codes of Practice? For example, the National Health Index Number and the Health Information Privacy Code?\(^{16}\)
- Are you taking reasonable precautions to ensure that you only assign unique identifiers to individuals whose identity is clearly established?

**If your agency:**

- uses another agency’s unique identifier without authority
- uses a ‘shared’ unique identifier in a way that breaches the requirements of a relevant Code of Practice
- Creates and assigns unique identifiers without meeting the requirement that they are *necessary* to the efficient functioning of your agency
- assigns the same unique identifier to two (or more) different individuals
- requires an individual to provide an unrelated unique identifier as proof of identity

*(Note: This principle cannot be overridden by the consent of the individual. That exception is deliberately not available. The responsibility rests solely with the agency.)*

**Then potential consequences are:**

- loss of reputation, trust and confidence in your agency and in other government agencies if the Privacy Commissioner decides your use of a unique identifier in a breach of Principle 12 of the Privacy Act.
- a breach of this principle could result in major system and process redesign and rebuilding and significant consequences for business operations.

**What could be done to reduce the risk?**

- Do not assign unique identifiers to individuals unless you absolutely have to.
- Ensure you know the identity of customers before you assign a unique identifier to them.
- Never use another agency’s unique identifier unless you are sure your use is authorised or your use is compliant with the relevant Code of Practice.
Scenario
The agency wishes to improve its customer management systems. Some of the agency’s customers have the same first and last name. To address this issue, driving licence numbers are required from all customers and are entered into the agency’s systems to uniquely identify the agency’s customers.

Breach of Principle 12
The agency has required individuals to disclose their driving licence numbers and is using it as their customer number.

Responding to the issue
• The agency should immediately cease requiring the driving licence number.
• The agency should also delete the driving licence numbers from existing records and, if a unique identifier is necessary to enable the agency to carry out its functions, it should create its own and put in place processes that ensure it is managed properly.
• The agency should identify what other information is available or could be collected from customers to help distinguish between people with the same names (e.g., street address, email address etc.).

What should be done to prevent this happening in the future?
• Ensure that policies and processes that deal with handling of personal information include the appropriate use of unique identifiers.