PRIVACY 101:

AN INTRODUCTION TO THE PRIVACY ACT

Participant Guide
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workbook layout</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>The Office of the Privacy Commissioner</td>
<td>6</td>
</tr>
<tr>
<td>The Privacy Act 1993</td>
<td>8</td>
</tr>
<tr>
<td>The aim of the Privacy Act</td>
<td>8</td>
</tr>
<tr>
<td>The principles of the Privacy Act</td>
<td>9</td>
</tr>
<tr>
<td>Definition of ‘personal information’</td>
<td>12</td>
</tr>
<tr>
<td>Definition of ‘agency’</td>
<td>13</td>
</tr>
<tr>
<td>The role of privacy officers</td>
<td>15</td>
</tr>
<tr>
<td>Privacy Act and Official Information Act</td>
<td>18</td>
</tr>
<tr>
<td>Section 7 overrides</td>
<td>20</td>
</tr>
<tr>
<td>Principle 1 - purpose for collection</td>
<td>22</td>
</tr>
<tr>
<td>Setting your purpose and being open about it</td>
<td>22</td>
</tr>
<tr>
<td>Principle 2 - source of information</td>
<td>26</td>
</tr>
<tr>
<td>Some exceptions to principle 2</td>
<td>28</td>
</tr>
<tr>
<td>Principle 3 - what to tell an individual</td>
<td>32</td>
</tr>
<tr>
<td>Principle 3 statement</td>
<td>33</td>
</tr>
<tr>
<td>Some exceptions to principle 3</td>
<td>37</td>
</tr>
<tr>
<td>Principle 4 - manner of collection</td>
<td>38</td>
</tr>
<tr>
<td>Collection principles summary</td>
<td>40</td>
</tr>
<tr>
<td>Key concepts</td>
<td>43</td>
</tr>
<tr>
<td>Principle 5 - storage and security</td>
<td>45</td>
</tr>
<tr>
<td>Physical and operational security</td>
<td>46</td>
</tr>
<tr>
<td>Transmission and disposal (or destruction)</td>
<td>48</td>
</tr>
<tr>
<td>Data breach</td>
<td>52</td>
</tr>
<tr>
<td>Dealing with a data breach</td>
<td>53</td>
</tr>
<tr>
<td>Containment / assessment and evaluation of risks</td>
<td>54</td>
</tr>
<tr>
<td>Notification and prevention</td>
<td>56</td>
</tr>
<tr>
<td>Principle</td>
<td>Page</td>
</tr>
<tr>
<td>-----------</td>
<td>------</td>
</tr>
<tr>
<td>Principle 6 - access</td>
<td>59</td>
</tr>
<tr>
<td>Requests</td>
<td>60</td>
</tr>
<tr>
<td>Procedural provisions</td>
<td>60</td>
</tr>
<tr>
<td>Timeframes for response</td>
<td>64</td>
</tr>
<tr>
<td>Charging</td>
<td>64</td>
</tr>
<tr>
<td>Some withholding grounds</td>
<td>66</td>
</tr>
<tr>
<td>Principle 7 - correction</td>
<td>72</td>
</tr>
<tr>
<td>Principle 8 - accuracy</td>
<td>75</td>
</tr>
<tr>
<td>Principle 9 - retention</td>
<td>78</td>
</tr>
<tr>
<td>Retention times and legal obligations</td>
<td>79</td>
</tr>
<tr>
<td>Principle 10 - use</td>
<td>82</td>
</tr>
<tr>
<td>Some exceptions to principle 10</td>
<td>83</td>
</tr>
<tr>
<td>Principle 11 - disclosure</td>
<td>85</td>
</tr>
<tr>
<td>Some exceptions to principle 11</td>
<td>86</td>
</tr>
<tr>
<td>Principle 12 - unique identifiers</td>
<td>91</td>
</tr>
<tr>
<td>Interference with privacy</td>
<td>93</td>
</tr>
<tr>
<td>Complaints about information privacy requests</td>
<td>94</td>
</tr>
<tr>
<td>All other complaints</td>
<td>95</td>
</tr>
<tr>
<td>Complaint intake process</td>
<td>100</td>
</tr>
<tr>
<td>Complaints process</td>
<td>102</td>
</tr>
<tr>
<td>Notes</td>
<td>106</td>
</tr>
<tr>
<td>Glossary</td>
<td>107</td>
</tr>
<tr>
<td>Additional resources</td>
<td>109</td>
</tr>
<tr>
<td>Appendix</td>
<td>110</td>
</tr>
</tbody>
</table>

The Privacy Act principles: quick reference guide | 110 |
Workbook layout

This workbook contains several types of study material, as indicated by the following icons.

Key point
This may include definitions, interesting points or where to find extra information. It will also show the steps that MUST be taken. They are very important for your learning, and to follow the law.

Key question
This introduces questions to reflect on or discuss through each section.

Insights for agencies
This shows some key information and advice for agencies from experts and other agencies.

Self-check activity
This activity provides an opportunity to reflect on your own organisation and to practise and evaluate your own understanding of the material.

Group activity
This activity provides an opportunity for you to interact within a group. It could be a discussion in pairs or a brainstorm or activity in a larger group.

Case note
This is a description of a real life example, to show how the theory being taught may be applied in practice.
Introduction

The Privacy Act 1993 regulates the way that agencies deal with personal information (sometimes referred to as ‘personal data’). A good rule of thumb to keep in mind when considering how the Privacy Act applies is to ‘put yourself in the shoes’ of the individual concerned and to think about how you would like your own information to be treated.

This material aims to introduce you to key concepts and definitions contained in the Privacy Act, including a brief discussion about the interface between the Official Information Act (OIA) and Privacy Act. This workbook will then focus on the 12 information privacy principles contained in the Privacy Act and will consider how they apply in practice. Finally, we will also look briefly at the consequences if there is a breach of the Privacy Act, including the test for an ‘interference with privacy’, the complaint process followed by the Office of the Privacy Commissioner (OPC) and possible court proceedings.

Because every case is different, this material is not designed to provide an exact answer about what view the OPC will form on a particular set of facts. However, this workbook will help you to recognise what parts of the Privacy Act will be relevant in the circumstances.

Figure 1 - Consider how you would want your information used
1. Follow the directions of your facilitator to introduce yourself by giving:
   · your name
   · your agency / role / position
   · what kind of privacy issues arise in your work
   · what you are hoping to get out of the session

2. Use this space to make notes of people’s names, and any privacy issues you had not previously thought of.
The Office of the Privacy Commissioner

Key question

What is the OPC?

The OPC is an Independent Crown Entity which means that it is not a direct part of the government. This is important because the OPC enforces the Privacy Act and investigates public sector agencies and so it needs to be independent of them.

Figure 2 - The OPC assists with investigation, conciliation and analysis

As well as the Commissioner, there are around 30 employees at the OPC which cover the roles of policy, investigations, communications and administration.

Key point

You may often hear the Office of The Privacy Commissioner called the ‘OPC’ or just ‘the Office’.
Key question

What does the OPC do?

The Office has a wide range of functions which include:

- **advice** - sharing information and advice with agencies and individuals
- **education and awareness** - running education seminars and workshops to promote awareness of the Act and how it operates
- **monitoring technological change** - monitoring and examining the impact that technology has upon privacy
- **monitoring data** - monitoring data-matching programmes between government departments
- **examining new legislation** - keeping up with the possible impact of new laws on individual privacy
- **making laws** - developing Codes of Practice for specific industries or sectors; checking draft legislation
- **investigations** - investigating complaints about breaches of privacy

![Diagram of OPC functions](image-url)
The Privacy Act 1993

The Privacy Act is the piece of legislation (law) that deals with the privacy of personal information or data. The Privacy Act is not about physical intrusions on privacy (such as someone looking in your bedroom window).

The Act also sets out the rules for information matching and provides a set of principles regulating the use of public registers. The principles are enforceable by complaining to the Privacy Commissioner.

There are also special ‘Codes of Practice’ that apply only to certain industries, such as health, telecommunications, and credit reporting. There are 12 principles, which are discussed in this material.

Insights for agencies

The term ‘data’ is not helpful and can invite complacency because it makes people forget that it is information about people.

The aim of the Privacy Act

What is the aim of the Privacy Act?

The aim of the Privacy Act is to give individuals more control over their personal information. The Act requires that when agencies are going to be collecting, holding and using personal information, that they are clear about what they are doing and why. The Act also provides individuals with the right to access and correct that information.

The focus of the Act is on purpose not consent. So, when an agency collects personal information, if it intends to disclose (tell another personal or agency) the information, for whatever reason, it needs to make the individual aware of this.

Once it has done so, and the individual then chooses to provide the information, the agency is free to disclose the information if it wants to; it doesn’t require any further authorisation from the individual concerned.
The principles of the Privacy Act

Key question

What are the 12 principles of the Privacy Act?

There are 12 information privacy principles that deal with how personal information is treated. These principles cover the collection, storage, use and disclosure of personal information, and give people the right to access and correct their information.

The Commissioner can issue industry-specific Codes of Practice, which modify the 12 information privacy principles to deal with specific types of information in a way that fits well with the particular industry. The main codes are:

- Health Information Privacy Code (HIPC)
- Telecommunications Information Privacy Code
- Credit Reporting Privacy Code

Key point

There are twelve principles that deal with how private information can be collected, stored, used and disclosed. If one of these principles is breached, a complaint may be made to the Privacy Commissioner.
Figure 4 - The principles of the Privacy Act
A general summary of the principles

The 12 principles have, in very general terms, the following effect:

<table>
<thead>
<tr>
<th>Principle</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principle 1 - purpose for collection</td>
<td>Only collect information when you need it for a lawful purpose connected with your agency.</td>
</tr>
<tr>
<td>Principle 2 - source of information</td>
<td>Obtain the information directly from the person concerned if possible.</td>
</tr>
<tr>
<td>Principle 3 - what to tell an individual</td>
<td>Tell the person what you are doing.</td>
</tr>
<tr>
<td>Principle 4 - manner of collection</td>
<td>Do not use unfair or unreasonably intrusive means of collecting the information.</td>
</tr>
<tr>
<td>Principle 5 - storage and security</td>
<td>Take care of the information once you have obtained it.</td>
</tr>
<tr>
<td>Principle 6 - access</td>
<td>The person can ask to see the information.</td>
</tr>
<tr>
<td>Principle 7 - correction</td>
<td>The person can ask you to correct the information.</td>
</tr>
<tr>
<td>Principle 8 - accuracy</td>
<td>Make sure that the information is accurate before you use (process) it.</td>
</tr>
<tr>
<td>Principle 9 - retention</td>
<td>Dispose of the information once you have finished with it.</td>
</tr>
<tr>
<td>Principle 10 - use</td>
<td>Only use the information for the purpose for which it was obtained.</td>
</tr>
<tr>
<td>Principle 11 - disclosure</td>
<td>Only disclose the information if this was the reason for which you obtained it.</td>
</tr>
<tr>
<td>Principle 12 - unique identifiers</td>
<td>Only use unique identifiers in place of person’s name where necessary.</td>
</tr>
</tbody>
</table>

Table 1 - A general summary of the Privacy Act principles
The information life cycle

As you will see, a piece of information has a life cycle involving:

- what you need to think about before you collect personal information
- what you need to consider once you have obtained the information
- what you need to take into account when you are using or disposing of the information

For example, if you are going to collect information, the Act tells you that the first thing you must do is decide why you need the information (principle 1). If you know why you are collecting the information, you can then tell the person concerned why you need it (principle 3). You are then able to use (or disclose) the information for that purpose (principles 10 and 11).

Definition of ‘personal information’

The Act applies to personal information about an identifiable individual. The Act defines the word ‘individual’ as a natural person (as opposed to a body corporate or company) other than a deceased natural person. (Note, however, that the Act can consider information about a deceased natural person in limited circumstances. See rule 11 (HIPC) and section 29(1)(a) of the Privacy Act.

If an individual is not identifiable, then the Act will not apply. However, care needs to be taken when ‘anonymising’ information, as simply removing someone’s name may not mean that the information is no longer identifiable. As an example, in some circumstances a description of a disease or set of events will be enough for someone to identify who is being discussed, even if their name is not used.

The word ‘information’ is not defined in the Privacy Act, but the High Court has said that it is not confined to the written word, but embraces any knowledge however gained or held, and, in some circumstances, can extend to information held in the mind of an individual.

As such, information about an individual could include written notes, emails, audio and CCTV recordings, photos or a summary of comments made about the individual during a recent discussion.

Figure 5 - Personal information is information about an identifiable individual
Definition of ‘agency’

The Privacy Act applies to agencies, not individuals. The word ‘agency’ is broad and covers any person or body of persons whether corporate or not and whether in the public or private sector.

Exceptions

There are some agencies that are not covered by the Privacy Act. Some examples are (this is not a complete list):

- members of Parliament in their official capacity
- courts / tribunals in relation to their judicial function
- news media in relation to their news activities

An agency has a responsibility to ensure that its employees adhere to the Act. Therefore, the agency is deemed to be responsible for any actions an employee takes in the course of their employment, or if an employee uses personal information they obtained in the course of their employment. However, the agency will have a defence if it can show that it did everything reasonable to prevent its employee from acting in this way. In such cases, the individual may be held directly liable.

Key point

More information on the defence that the agency did everything possible to stop a breach action, and is therefore not liable, can be found in section 126 of the Act.

The principles generally do not apply to information held or used in connection with your personal, family or household affairs. It is only if you obtain a piece of information through your employment that the Privacy Act will apply, so you need to treat the information differently to how you would treat information gained from your friends or family.

However, if you collect, use or disclose personal information in a way which would be highly offensive to a reasonable person, then the principles may apply even if you collected, used or disclosed that information in a personal capacity.
Key point

An agency can be:
- any person or group of people
- in the public or private sector

Some common examples of exceptions:
- Members of Parliament (MPs)
- courts and tribunals
- news media in relation to their news reporting activities

Agencies are normally responsible for their employees’ actions (sections 3-4; defence section 126).

Personal information relating to domestic affairs is only covered by the Act if the collection, use or disclosure of that information would be highly offensive to a reasonable person (section 56).
The role of privacy officers

The Privacy Act, section 23 states that every agency must appoint a privacy officer. The privacy officer is responsible for:

- ensuring that the agency complies with the Act
- dealing with requests made to the agency for access to, or correction of personal information
- working with the Privacy Commissioner’s Office when it investigates complaints

To do this, the privacy officer needs to be familiar with the Privacy Act and the agency’s obligations under the Act, as they apply to their agency.
Self-check activity

Answer the questions below about the privacy officer at your agency. If you are your agency’s privacy officer, reflect on the questions and answer them according to your own role.

1. What is the privacy officer’s name?

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

2. How are the privacy officer’s contact details communicated:

a) to agency staff?

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

b) to the public?

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

3. What do I know about the responsibilities of the privacy officer’s role?

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________
4. What tasks has the privacy officer completed within their role?

________________________________________________________

________________________________________________________

________________________________________________________

5. Has the privacy officer assisted with an OPC complaint?

________________________________________________________

________________________________________________________

________________________________________________________

**Insights for agencies**

Make sure you have a privacy officer in your agency who staff can contact to notify of any suspicion or threat of a data breach.
Privacy Act and Official Information Act

The Privacy Act applies to public and private sector agencies and gives an individual (or their agent) the right to request any information the agency holds about them.

The Official Information Act (OIA) applies to public sector agencies and gives individuals and organisations the right to request any information (which may include information about other people). It is important to note that the OIA could apply to a private sector agency where that agency is contracted to work on behalf of a public sector agency.

If you receive a request for information from someone who is not:

1. the individual concerned or their agent, or
2. the individual’s representative

and you are a public sector agency, you must consider the request under the OIA.

The OIA requires disclosure unless there is good reason for withholding information. Section 9(2)(a) of the OIA provides that information can be withheld if it is necessary to protect the privacy of a natural person including that of a deceased natural person.

This requires a balancing exercise between the privacy interests of the individual and the public interest in disclosure. The request does not have to be in writing. However, the OPC recommends that you either ask for it in writing, or make a note of the request in writing yourself, in order to avoid any disputes at a later date.

If information is not held by your agency, but you know who does hold it, it must be referred within 10 working days (section 14 of the OIA).
Key point

The Privacy Act applies to information you hold about the individual requesting the information.

The Official Information Act applies to information that the requester asks for about someone else from a public sector organisation.

Figure 7 shows how the Privacy Act and the Official Information Act work with each other, and is a helpful tool when determining which Act applies.

Privacy Act and OIA Interface

Requester asks for information about himself or herself

Privacy Act
Principle 6. withholding grounds under sections 27-29 may apply

Official Information Act
Section 5 - presumption of availability
Unless good reason for withholding information
Section 9(2)(a) withholding ground which protects the privacy of natural persons

Requester asks for information about someone else from a public sector agency

Figure 7 - How the Official Information Act and the Privacy Act work with each other
Section 7 overrides

Section 7 of the Privacy Act states that other statutes which prohibit or restrict the availability of personal information take precedence over the information privacy principles. Section 7 also recognises that where another piece of law allows or requires personal information to be used in a specific way, this will override the general provisions of the Privacy Act. When this happens, the OPC calls it a section 7 override.

For example:

- The Tax Administration Act allows or requires the IRD to collect and disclose information in a certain way.

- ACC can only collect information with the patient’s authorisation.

- Section 11 of the Social Securities Act lets the Ministry of Social Development collect specific types of information, as long as certain conditions are met.

- Several Acts in the health context, such as the Cancer Registry Act, Mental Health (Compulsory Assessment and Treatment) Act, and so on, are also included in this category.

**Key point**

A section 7 override is where another piece of law allows or requires personal information to be used in a specific way. This will override the general provisions of the Privacy Act.
Group activity

1. Use the space provided to write any notes or questions.
Principle 1 - purpose for collection

Key point

Principle 1

Personal information must only be collected when:
- the collection is for a lawful purpose
- the purpose is connected with the functions of the agency, and
- it is necessary to collect the information for that purpose

Setting your purpose and being open about it

Principles 1-4 of the Privacy Act concern the collection of personal information.

The Act states that agencies have to do the following two things:

1. Set a purpose - develop policies for collecting information.
2. Be open about it - tell individuals about those policies when they collect this information.

Agencies must not collect personal information from people unless:

1. the information is collected for a lawful purpose connected with a function or activity of the agency, and
2. collection is necessary for that purpose

Principle 1 is about what information an agency is allowed to collect. It is designed to stop agencies from collecting information that they do not need.

Key point

Principle 1 is written to stop the excessive collection of information. It is designed to encourage agencies to set a purpose and be open about it.
Understand the collection process

It is very important to understand the collection process, because it relates directly to the guidelines around how the information can be used and disclosed. The first step for an agency is to set its purpose in compliance with principle 1. Once an agency knows exactly what its purpose is for collecting personal information, this will enable the agency to properly communicate this purpose to individuals when it collects their information (principle 3) and then later uses or discloses this information (principles 10 and 11) in compliance with the Privacy Act.

Agencies must set their own purpose

To comply with principle 1, agencies must set their own purpose with regard to the information they collect. In doing so, the agency must ask itself the following question:

Do I have a lawful purpose for collecting the information?

In order to answer this question, the agency must consider the following things:

- **What** information do I need to collect?
- **Why** do I need this information?
- Is there a law about **how** to do this?
- Is the **purpose** connected with a function or activity of the agency?
- Is the collection of this information **necessary** to achieve that purpose?

Many agencies fail on the last point. By failing to determine whether or not it is actually necessary to collect the information, you may end up collecting information **unlawfully**.
Principles 1-4 only apply when an agency **collects** personal information. While the term ‘collect’ has been given a broad meaning (‘gathering together; the seeking of or acquisition of personal information’), if an agency receives **unsolicited** information, then principles 1-4 will not apply.

As an example, if an agency received a tip-off that one of its employees was lying about being on sick leave when they were actually taking a holiday, along with photos of the employee from Facebook as proof, this would not raise issues under principles 1-4.

However, don’t forget that, no matter how the agency obtained the personal information, once it holds the information, the other principles (5-12) will still apply.

**Insights for agencies**

Develop simple and easy to understand policies and guidelines about privacy.
1. Follow the directions of your facilitator to form groups.
2. Complete the task as directed by your facilitator.
3. Use the space provided to write any notes or questions.
Principle 2 - source of information

Principle 2 relates to the sources from which an agency can collect personal information.

When collecting information or planning to collect information, ask yourself the following:

1. If you want to collect information about an individual, who is the best person to collect that information from?

2. Under what circumstances might you need to collect it from someone else?

Generally, personal information should only be collected from the individual concerned. This ensures that the person knows that information is being collected from them. They also know what information is being collected, and have the opportunity to exert some control over what is collected.

Key point

Principle 2

Personal information must usually be collected from the person who the information relates to. But the Privacy Act does allow you to collect information from other people in limited cases, for instance, when:

- the person concerned authorises collection from someone else
- obtaining it from the person concerned would undermine the purpose of the collection
- this is necessary in order for a public sector body to uphold or enforce the law
- this is necessary for the purposes of court or tribunal proceedings
Group activity

1. Follow the directions of your facilitator to form pairs or small groups.
2. Discuss examples of when an agency might want to collect information from people other than the individual concerned.
3. Use the space provided to write any notes or questions.
Some exceptions to principle 2

There are a number of cases where your agency will be permitted to collect personal information from someone other than the individual concerned. A full list of exceptions can be found in the Act, but some of the more commonly used exceptions are:

1. **Compromise to collection** - where collecting information from the person directly may prejudice the purpose of collection.

2. **Compromise to safety** - where collecting information from the person directly may prejudice the safety of any person (this could include the person asking for the information or the person that the information is about).

3. **Authorisation given** - where the individual has authorised (allowed) collection from someone else. If asking for authorisation from an individual, you should make sure they understand:
   a) what is to be collected
   b) from whom it is to be collected (collection may be restricted to one particular person)
   c) the purposes for obtaining the information, and
   d) who will receive it

   The extent of the authorisation should be clearly understood. Safeguard yourselves by requiring the authorisation to be explicit, clearly defined and, if possible, in writing, so that if any problems arise at a later date a written record of what was agreed to

4. **Individual not identified** - if no one can find out who the person is, and information is used for statistics and research purposes. Non-compliance is also permissible where the information will not be used in a way that identifies the individual, e.g., it is only statistical information, and all identifying information has been removed.

5. **Not reasonably practical** - compliance is not reasonably practicable in the circumstances.

6. **Necessary for court proceedings** - the individual is not considered legally competent.

These exceptions may also be relevant for things like detecting theft and fraud. In such situations, if your agency told people why you were collecting the information, they might modify their **behaviour**. Without information from another source, of which the person is unaware, you could not collect the information necessary to charge them.
Key point

If information is collected from someone other than the individual themselves, it is a good idea to note it on the file. If appropriate, you may wish to check the accuracy with the individual in order to make sure you are in compliance with principles 7 (correction) and 8 (accuracy).
1. Follow the directions of your facilitator to form pairs or small groups.
2. Complete Table 2 as directed by your facilitator.
3. Use the space provided to write any notes or questions.

<table>
<thead>
<tr>
<th>Exception</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compromise to collection</td>
<td></td>
</tr>
<tr>
<td>Compromise to safety</td>
<td></td>
</tr>
<tr>
<td>Authorisation given</td>
<td></td>
</tr>
<tr>
<td>Individual not identified</td>
<td></td>
</tr>
<tr>
<td>Not reasonably practical</td>
<td></td>
</tr>
<tr>
<td>Necessary for court proceedings</td>
<td></td>
</tr>
</tbody>
</table>

Table 2 - Exceptions to principle 2
A job applicant nominates a referee from her previous job to be contacted by a potential employer. The employer relies on a recruitment agency to screen employees. The recruitment agency fails to note that the employer was only authorised to contact a particular referee at the company.

As a result, the agency obtained an adverse reference from a manager with whom the applicant had had a bad relationship. As a result, the recruitment agency did not recommend the individual and an offer of employment was withdrawn.

The applicant had alerted the employer to this negative relationship, but because the screening agency obtained the reference in confidence and only gave the employer a recommended or not recommended result, the employer was not aware that the reference had been obtained from an unauthorised (not allowed) referee.

Key point

When sourcing personal information for your agency’s purpose, ensure that you only collect information from the individual concerned, unless an exception applies.

The test for believing that an exception applies is reasonable grounds. What is considered ‘reasonable’ will depend on the circumstances.

It is up to the agency to establish whether reasonable grounds exist (section 87), so it is best to document why you believe the exception to apply.

Case note: unauthorised referee

A job applicant nominates a referee from her previous job to be contacted by a potential employer. The employer relies on a recruitment agency to screen employees. The recruitment agency fails to note that the employer was only authorised to contact a particular referee at the company.

As a result, the agency obtained an adverse reference from a manager with whom the applicant had had a bad relationship. As a result, the recruitment agency did not recommend the individual and an offer of employment was withdrawn.

The applicant had alerted the employer to this negative relationship, but because the screening agency obtained the reference in confidence and only gave the employer a recommended or not recommended result, the employer was not aware that the reference had been obtained from an unauthorised (not allowed) referee.
Principle 3 - what to tell an individual

Key point

Principle 3

When an agency directly collects personal information, it has to take reasonable steps to make sure that person concerned knows things like:

- why it is being collected
- who will see the information
- whether the person is required to give the information or whether it is voluntary
- what will happen if the information isn’t provided

Again, there are sometimes good reasons for not letting a person know. For example, it could undermine the purpose of the collection, or it is just not possible to tell the person.
When you are collecting information from people, be open about it. Tell them why. It may be useful to think about what you would like to know before you handed over your personal information. A ‘no surprises’ basis is best!

Tell people the following:

1. why you are collecting the information (the purpose)
2. who will see the information
3. whether the supply of information is voluntary (they can choose whether or not to give it) or mandatory (they must give the information)
4. the consequences (what will happen) if information is not supplied
5. the person’s rights of access (to see the information or obtain a copy) and correction (to change the information)

Take reasonable steps to ensure that people are aware of what information you are collecting and why you are collecting it. This will help to prevent any misunderstandings, and can be critical later when you use or disclose the information. If you know that you are going to disclose the information because that is your purpose, then say so.

This information forms what the OPC calls a principle 3 statement. The information can be conveyed in a number of ways, including:

- telling the person in a language that they understand
- putting notices or signs on display
- providing letters and brochures, or including statements on the form to be completed

It is important that the person’s attention is drawn to this information. If the information is provided on a form to be completed by the person, they should be able to either take a copy with them or access the information elsewhere, e.g., on your agency’s webpage.
Being open

You need to tell people all of the following:

The fact that information is being collected

It is not always obvious that information is being collected or that it is being collected in a particular way, so don’t assume people know. If an audio or video recording is being made, is the recording equipment in plain view, and has it been pointed out to them?

The purpose for collection

Give a good indication of why information is being collected and what it will be used for. If you only tell the person a very small part of what the information will actually be used for, this could cause problems for your agency when you try to use it later on. However, if the purposes that you give are too broad, then informing the person will become pointless.

Always be aware that the less obvious purposes are the ones that could cause people distress. So make sure that you tell people about these ones particularly. The following case note is a medical example that illustrates this point well.

Case note: use of religious information

It is common practice for hospitals to ask for the religion of patients. It is not always apparent why this information is required. Often there is no other reason for asking except to inform the hospital chaplain. However, when individuals are not told there can be unanticipated adverse consequences.

In one case investigated by the Office, a 16-year-old girl was admitted for a termination. She indicated on her admission form that she was Catholic. While she was there for the procedure, she was visited by the chaplain who observed from her notes that she had been admitted for a termination.

The chaplain relayed this information to her parents. Had the hospital phrased its request in terms of: ‘If you would like to be visited by a chaplain, please indicate your religion,’ this situation could have been avoided.
Who will see the information

Individuals should be told of the agency’s practices and anticipated disclosures. You don’t need to tell them about absolutely every possible disclosure - just give a general indication of who is likely to see the information and the reasons they will need to see it. In the above case note, clinical staff are obvious recipients, but researchers, students and hospital chaplains would not be.

In a business context, you should say if you are going to pass the information onto other companies for marketing purposes. For the sake of clarity, it may be best to let people know when you intend to pass information on to any other businesses, even where they are subsidiary companies or part of the same retail chain.

The contact details for the agency collecting and holding the information

Some agencies may collect information on behalf of another agency. If the information will be held by an agency other than the one collecting the information, you must let the person know who will be in charge of the information.

Whether the supply of information is voluntary or mandatory

Where your agency is relying on another specific piece of law to collect personal information, you need to let people know:

1. what the piece of law is; and
2. whether they have a choice to tell you the information or not

Some laws will allow agencies to collect certain personal information but do not oblige the individual to provide the information if they don’t want too. However, other laws will state that individuals are required to provide information and could, for example, be fined if they don’t.

The consequences of not providing the information

Tell the person what will happen if they do not provide the information. For example, it might not be possible to process a person’s application, subsidy or benefit. In a medical context, the agency might state that a treatment might not be as effective, or could be fatal, without the correct information.

Rights of access and correction under principles 6 and 7 of the Act

You need to let the person know that they have the right to ask to see the information you have collected, and to request its correction if necessary.
Key point

Best practice is to provide all the principle 3 statement information (if practicable) before the collection of information.

Group activity

1. Use the space provided to write any notes or questions.
Some exceptions to principle 3

Key question

When might you not want to tell people or make them otherwise aware that you are collecting information from them?

There are some cases where agencies will not need to provide the individual with a principle 3 statement. This is where the agency believes on reasonable grounds that an exception applies. A full list of the exceptions can be found in the Act, but some common examples are:

- It is not reasonably practicable in the circumstances.
- It may prejudice the purpose of collection or maintenance of the law, or the safety of any person (for example, covert camera surveillance).

This is very similar to principle 2 and there are the same types of exceptions. You must also believe on reasonable grounds that the exceptions apply. Again, as per section 87, if your agency relies on an exception, then the burden is on you to show why the exception applied. To make this easier, the agency should document why it believes an exception applies as and when such an occasion arises.

If it is not practicable to give an explanation at the time, then as soon as possible afterwards is acceptable. It is not necessary to repeat the explanation every time information is collected from an individual for the same purpose. However, if your principle 3 information has changed, or if it has been a while since you’ve dealt with someone, you should give them a refresher.
Principle 4 - manner of collection

**Key point**

**Principle 4**

Personal information must not be collected by unlawful means or by means that are unfair under the circumstances or unreasonably intrusive.

Personal information must **not** be collected by means that are:

- unlawful
- unfair under the circumstances, or
- unreasonably intrusive

The focus of principle 4 is on the manner in which information is collected, rather than what is collected (i.e., **how** rather than why the information is collected). An explanation of the terms and an example of each is shown in Table 3.

<table>
<thead>
<tr>
<th>Term</th>
<th>Explanation</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unfair</td>
<td>Includes misleading the individual as to the purpose of collection, or using threats or coercion to obtain information</td>
<td>Debt collection agencies pretending to be someone else in order to find out a person’s whereabouts.</td>
</tr>
<tr>
<td>Unreasonably intrusive</td>
<td>When considering what may be regarded as unfair or unreasonably intrusive, the agency should ask: What is it about these circumstances that justify the means used to collect the information? It’s also helpful to think about how you would feel if your information was being collected in this way.</td>
<td>Installing cameras in a changing room.</td>
</tr>
</tbody>
</table>

Table 3 - Principle 4 breaches
A man became aware that his local pub had CCTV operating in the men’s restroom after seeing a still taken of him using the facilities. He complained this was an intrusive collection.

The pub manager informed us that CCTV was in operation in the pub for safety and security reasons, and confirmed the pub did have signage about the use of CCTV (although nothing explicitly said that cameras were operating in the bathroom).

We considered that general use of CCTV was reasonable as there was signage, the footage was only used for safety and security, and there was adequate protection of the information (for example only certain staff could access it).

However, we were not satisfied there was a good reason to have a camera operating in the toilet given that it was capturing highly sensitive information. On this basis, we considered that the pub had breached principle 4.

Based on our view the pub manager agreed to remove the camera from the toilet area.
Collection principles summary

Principles 1-4 state that you need to decide and communicate:

- why you are collecting information - purpose
- who you are collecting it from - source
- what you tell people when you collect their information
- how you collect information

Figure 8 - You need to tell people who will view their information

Key point

If you receive unsolicited information, the collection rules don’t apply.
1. Follow the directions of your facilitator to form pairs or small groups.
2. Complete the task as directed by your facilitator.
3. Use the space provided to write any notes or questions.
A man applied for trauma insurance, providing extensive medical information and authorising the insurance company to collect health information relating to the application and any previous claims. The insurance company contacted the man’s GP and obtained the man’s full medical history for the preceding five years.

When we investigated the complaint, the insurance company advised it had identified three issues in the application about which it needed further information.

We formed the view that the company should only have requested information relating to the three issues and that, as a result, it had breached rule 1 of the HIPC by collecting five complete years of the man’s medical history.

The insurance company accepted our view and amended its process so that it only asks for information relating to the specific conditions identified in applications. It also reached a confidential settlement with the complainant.

Reflection

Use the space provided to create a mind map of the concepts you have learnt so far about the fair collection of personal information.
Key concepts

Keep in mind the following key concepts when collecting personal information:

- Having a **clear purpose** allows the agency to ask the right questions to collect the necessary information.

- Principle 1 links into other principles, so that if an agency has made a good attempt at explaining its purpose, as required under principle 3, people are more likely to understand why the collection of information is necessary and how the information will be used and disclosed (principles 10 and 11).

- Defining or setting your purpose is important, as it will limit the manner in which the information to be collected can be used or disclosed.

### Key point

The Act says that all agencies **must**:

- develop information-handling policies
- tell people about these policies when they are collecting information

Setting your **purpose** and being **open** about that purpose is a very important part of understanding and applying the Act.
Group activity

1. Follow the directions of your facilitator to form pairs or small groups.
2. Complete the task as directed by your facilitator.
3. Use the space provided to write any notes or questions.
Principle 5 - storage and security

Key point

Principle 5

It is impossible to prevent all mistakes. But any agency must ensure that it takes reasonable steps to prevent the loss, misuse or disclosure of personal information.

Principle 5 requires agencies to take reasonable security safeguards to protect against:

- loss
- unauthorised access, use, modification, or disclosure; and
- other misuse

What is reasonable will depend on the nature of the information being held and the potential risk of harm occurring. Financial information is generally considered to be sensitive.

Also, keep in mind that the agency is responsible for the personal information it holds directly and all personal information that it provides to any individual or agency acting on its behalf. So, if an agency has to give information to someone else to allow a service to be provided, it must do everything reasonable within its power to prevent the unauthorised use or disclosure of that information by the recipient.

Insights for agencies

Carry out regular audits of your agency’s IT security. Employ an IT security company to conduct penetration tests on your system to look for security flaws. Fix any weaknesses that are identified.

Have a notice counting the days since the last data breach and celebrate as an agency when the time elapsed breaks a previous record.
Physical and operational security

As an agency you are in the best position to determine the risk of harm occurring and the steps that can be taken to reduce that risk.

Below are some of the steps you should consider taking when developing a storage and security policy.

**Physical security**
- Implement a clear desk policy.
- Lock information away.
- Restrict unauthorised access.
- Turn computer screens and whiteboards away from public areas.
- Place computers, faxes and printers where they cannot be accessed by unauthorised personnel.

**Electronic security**
- Have appropriate firewalls.
- Install and update antivirus software.
- Update passwords regularly.

**Operational security**
- Restrict staff access to information - only allow access to information that staff need to do their jobs. This can be done physically, electronically or through the separation of files, e.g., separating personnel files into accounts, medical and performance.
- Run staff training covering:
  - the need for security for client or personnel records
  - when information may be accessed, used and disclosed
  - warnings against ‘employee browsing’ (unauthorised access of files)

**Key point**
Staff training is a key requirement under principle 5 of the Act.
Insights for agencies

Develop a whole-organisation approach to privacy, one that values personal information and treats it with care. For example, privacy is not just the responsibility of an agency’s legal department, because it also involves information technology, human resources and other areas.

Accountability structures need to be clear so top and senior management recognise that they are ultimately responsible for information breaches.

Where an information system is broken, shutting it down is a drastic resort but may work in some cases to prevent a wider breach.

Figure 9 - Good security practices protect your agency and individuals
Transmission and disposal (or destruction)

Transmission

Transmission of information includes the following measures.

- Implement controls on the type of information that can be sent by fax and / or e-mail.
- When using a facsimile, make a telephone call prior to transmission to ensure that the information is uplifted immediately.
- If you are relying on a contractor for information handling, have an agreement with the contractor that only duly authorised staff can access records.
- When using e-mail, use ‘nicknames’ or an address book to send information to minimise inadvertent disclosure. Encryption is something else that you may consider. You should consider turning off ‘auto-complete’ or using the ‘delay delivery’ function. You should also have clear policies around the type of information staff may or may not send by email.

Disposal

When information is no longer needed, it must be disposed of in an appropriate manner. Disposal of information could involve things like:

- using a shredder
- if using an outside contractor, making the secure destruction of documents a condition of the contract

It is best practice to have a policy about how and when files will be disposed of.

Figure 10 - Have a policy about how and when files will be disposed of
Key point

When determining whether a security safeguard is reasonable, the Commissioner will consider:

- the sensitivity of the information
- where the information is located
- the likely harm that would occur if principle 5 was breached
- the steps and/or policies in place to guard against such a breach
- whether those steps and/or policies have been followed
- relevant training provided to staff
1. Follow the directions of your facilitator to form pairs or small groups.
2. Complete the task as directed by your facilitator.

### Security questions

<table>
<thead>
<tr>
<th>Consider the following scenarios.</th>
<th>What issues, if any, does the responsible agency need to consider?</th>
</tr>
</thead>
<tbody>
<tr>
<td>A debt collector faxes someone at work about an outstanding debt. The fax is given to another staff member via the internal mail system.</td>
<td></td>
</tr>
<tr>
<td>A doctor tells a patient their blood test results over the phone. They can hear other people in the background.</td>
<td></td>
</tr>
<tr>
<td>A bank sends a monthly statement through the mail but it is wrongly delivered to a neighbour, who later advises the intended recipient to change banks because he has much lower mortgage payments.</td>
<td></td>
</tr>
<tr>
<td>A couple visits the fertility clinic. At a family dinner a week later, a relative asks why they had not said they were attending the clinic. Her friend is the receptionist there.</td>
<td></td>
</tr>
<tr>
<td>A ‘process server’ gives a person notice that their ex-partner has commenced proceedings before the Family Court over access to the children. The person asks how the process server obtained their address, as they have recently moved, have a confidential phone number, and their address has been suppressed on public registers like the electoral roll. The process server tells the person that he purchased the name and address from a government department.</td>
<td></td>
</tr>
</tbody>
</table>

Table 4 - Security questions
3. Use the space provided to write any notes or questions.
**Data breach**

- **Key question**
  - What is a data breach?

  A data breach is when someone who should not have access to personal information sees it, either intentionally or by accident.

- **Key question**
  - How do data breaches happen?

  Data breaches happen in a number of ways, including:

  - **lost records and equipment** - lost or stolen laptops, USBs (memory sticks) or paper records
  - **incorrect e-waste disposal** - incorrect hardware disposal and return caused by computer hard disk drives being thrown away, recycled or returned to leasing companies, or serviced incorrectly, without the contents first being erased
  - **hackers** - illegal access of databases
  - **employee browsing** - accessing or disclosing personal information without authorisation
  - **document theft** - taken from recycling or rubbish bins
  - **information given to the wrong person** - information sent to the wrong physical or email address
  - **fraudsters** - releasing personal information to a person pretending to be someone else
Dealing with a data breach

Principle 5 is also the main principle which is engaged when there is a privacy (data) breach. There are four key steps an agency should take when something goes wrong with the personal information it holds.

Key steps: responding to a breach

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Containment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Contain the breach and make an initial assessment.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Evaluate the risks.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Notification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Notify affected people if necessary.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Prevention</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Prevent a repeat.</td>
</tr>
</tbody>
</table>

If you think there has been a breach, move quickly to investigate the breach and what harm it could do.

Think about these questions:

- What could happen to the people the information relates to - i.e., your customers, clients, suppliers, patients, etc.?
- What harm could this do to your organisation - e.g., a loss of public trust and / or damage to the organisation's reputation?

Steps 1, 2 and 3 should be undertaken either simultaneously (at the same time) or in quick succession (one after the other). Step 4 provides recommendations for longer-term solutions and prevention strategies. The decision on how to respond should be made on a case-by-case basis.
Containment / assessment and evaluation of risks

Breach containment and preliminary assessment

Once you have discovered, or suspect, that a privacy breach has occurred, you should take immediate common sense steps to limit the breach, for example:

- **Contain the breach** - Stop the unauthorised practice, recover the records, shut down the system that was breached, revoke or change computer access codes or correct weaknesses in physical or electronic security.

- **Designate an appropriate individual** - Someone should be appointed to lead the initial investigation.

- **Determine who needs to be made aware of the incident** - Decide who should be told what has happened. Escalate internally as appropriate and inform the person within your agency responsible for privacy compliance (typically the privacy officer).

- **Contacting authorities** - If the breach appears to involve theft or other criminal activity, notify the Police.
Evaluate the risks

To determine what other steps are necessary, you should assess the risks associated with the breach. Consider the following factors when assessing the risks:

- How sensitive is the information? Generally, the more sensitive the information, the greater the risk of harm to individuals.
- 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 a name, address and date of birth suggest a higher risk due to the potential for identity theft.
- To the extent possible, determine the cause of the breach.
- Is there a risk of ongoing breaches or further exposure of the information?
- Has the personal information been recovered?
- What steps have already been taken to mitigate the harm?
- How many individuals’ personal information was affected by the breach?
- What harm could result from the breach? Examples include:
  - a security risk, for example, physical safety
  - identity theft
  - financial loss
  - loss of business or employment opportunities, and / or
  - significant humiliation or loss of dignity, damage to reputation or relationships
Notification and prevention

Notification

Key question

Should affected parties be made aware of the breach? If so, how will you notify them?

If a privacy breach creates a risk of harm to the individual, they should be notified. Each incident needs to be considered on a case-by-case basis to determine whether privacy breach notification is necessary. Remember that it is currently voluntary whether you notify anyone of a privacy breach. Agencies are encouraged to inform the OPC of material privacy breaches so that it is aware of the breach and can effectively handle any related enquiries (questions) or complaints.

The key consideration in deciding whether or not to notify affected individuals should be whether notification is necessary in order to avoid or mitigate harm to the individual whose personal information has been inappropriately accessed, collected, used or disclosed. Agencies should also take into account the ability of the individual to take steps to mitigate any harm.

Consider the following factors when deciding whether to notify:

- Do you have any legal and contractual obligations?
- What is the risk of harm to the individual? Is there a risk of physical harm (if the loss puts an individual at risk of physical harm, stalking or harassment), or of identity theft or fraud?
- What is the ability of the individual to avoid or mitigate possible harm?

Notification to individuals affected by the breach should occur as soon as reasonably possible following the assessment and evaluation of the breach. The preferred method of notification is directly to affected individuals by phone, letter, email or in person.
Prevention

Key point

If a privacy breach creates a risk of harm to the individual, they should be notified.

For more information see the OPC’s Privacy Breach Guidelines and webpage entitled ‘Finding other people’s personal information’.

Key question

What lessons can be learned from this experience to prevent future breaches?

Agencies need to take the time to investigate the cause of the breach and consider whether to develop a prevention plan. The level of effort should reflect how serious the breach was, whether it involved the whole organisation or just one small part, and whether it would be likely to occur again or whether it was just a one-off event.

Insights for agencies

Make privacy and information security top priorities for your organisation. People need to have confidence that their personal information is protected.

Ensure that workers are getting training on how to respect people’s information, how to manage their data and how to prevent breaches.

Carry out spot audits on what information is being accessed, for what reasons and by whom.
Reflection

Use the space provided to create a mind map of the concepts you have learnt so far about data breaches.
Principle 6 - access

If information is readily retrievable people have a right to receive confirmation of whether or not an agency holds information about them (including information received from other agencies).

Key point

Principle 6
People have the right to ask for access to personal information about themselves.

Agencies can refuse to give access in some limited situations, for instance, where giving the information would:

- endanger a person’s safety
- prevent the detection and investigation of criminal offences
- involve an unwarranted breach of someone else’s privacy

Under principle 6 individuals are entitled to:

- know whether an agency holds information about them
- access that information if it is readily retrievable

There is a presumption of access. So if someone asks you for information you hold about them, it is presumed that you will provide it. There are also procedural provisions (what needs to be done and how) that you need to follow, including set timeframes. The procedural provisions are found in parts 4 and 5 of the Privacy Act.

However the right to access personal information is not absolute and an agency will be allowed to withhold personal information in limited circumstances. These withholding grounds are set out in sections 27-29 of the Privacy Act.

What will be regarded as readily retrievable will depend on the circumstances of the case. What is deemed retrievable may not be limited to written documentation and can extend to discussions.
Whenever an agency provides a decision in response to an information request, it must inform the individual of their:

- right to have the decision reviewed by the Privacy Commissioner, and
- right to request correction of any information they believe is incorrect, under principle 7 of the Act

**Requests**

There are a number of things to keep in mind when dealing with a request for personal information, including the following:

- Requests for information may be in written or oral form and individuals do not have to explain why they want their information.
- A request cannot be refused on the basis that the individual does not own the information. Equally, the right of access is not a right to possess original documentation.
- Information is not limited to written documentation, but can extend to information in the mind of an individual.
- Individuals can appoint agents. However, check that they are properly authorised to request access and that there is written authority (section 45).

**Procedural provisions**

Procedural provisions are what must be done by the agency and how it must be done. There is an obligation on an agency to:

- provide assistance
- transfer access requests
- inform the individual of the decision regarding their request
- respond within time limits
- make information available in the form requested
When an agency receives an access request, the Privacy Act means that you must do the following:

- **Provide assistance (section 38)**
  You must assist the individual making the request; this may include redirecting the individual to the appropriate agency, helping them to formulate a request or advising them of what information the agency holds. This also means you should be able to identify when someone is seeking information that they are entitled to request under the Privacy Act, even if they do not directly refer to the Act.

- **Transfer access requests (section 39)**
  Where you do not hold the information, but believe it to be held by another agency, you must transfer the request within 10 working days from receipt and inform the individual accordingly. You can also transfer a request where you do hold the information if the information is held by another agency and it is more closely related to that agency, e.g., where you have received a copy of a report from another agency.

- **Inform the individual of the decision regarding their request (section 40)**
  If you do not transfer the request, you must make a decision in relation to the request and inform the individual of this decision. Your decision should include whether you intend to make the information available in full, in part, or not at all, and - if the request is to be granted - the way in which the information will be made available. You must also inform the individual of the basis for withholding any information and their right to have your decision reviewed by the Privacy Commissioner.

  You do not have to provide the individual with the information at the same time as you make a decision (although this will generally be the case). However, if you do not provide the information at the same time, you must provide it **without undue delay**. (What is considered to be ‘undue’ will depend on what the information is and / or whether there is any particular reason for urgency, for instance, if the individual needs the information for an upcoming court case.)

- **Respond within time limits (sections 40-41)**
  Generally, unless you have transferred the request to another agency, you must inform the individual of your decision within 20 working days of receiving the request.
However, you may extend the timeframe for responding if:

- the request is for a significant amount of information or would require you to search through a large amount of information and this can’t reasonably be done within the original time frame, or

- you need to consult with someone before you can make a decision on the request (for instance, if you need to speak with a specific staff member or another agency) and you are not able to do so and still provide a response within the original time frame.

If you wish to extend the time frame for response you need to tell the individual about this within 20 working days of receiving the request and inform them of:

- the length of the extension, i.e., when you will be providing a response
  - the reasons for the extension, and
  - their right to make a complaint to the OPC about the extension

- **Make information available in the form requested (section 42)**

  This can be a copy, summary, viewing, etc. The information must be released as requested unless doing so would impair efficient administration or be contrary to any legal duty the agency had in respect of the document or prejudice the interests protected in sections 27-29.

The flowchart in Figure 11 sets out the steps that must be followed when responding to a request.
Individual makes a request for personal information under principle 6 of the Privacy Act

Before processing the request consider:
- Is the individual requesting ‘personal information’? (section 2)
- Does the individual require any assistance with making the request? (section 38)

Does your agency hold the requested information?

Yes

Can you make a decision about the information request within 20 working days? (section 40)

Yes

Do you know which agency does?

Yes

Transfer the request to the other agency within 10 working days, and tell the requester you have done so (section 39)

No

Let the requester know that you don’t hold the information within 20 working days

No

If you require more time to process the request, and meet the criteria, you should advise the requester that you require an extension (section 41)

Are you going to release the requested information, or do you want to withhold all, or some of it?

Releasing

You need to:
- Consider how to provide the information (section 42)
- Consider if you want, and are able, to charge for the information (section 35)
- Inform the requester of their right to request correction (principle 7)
- Release without undue delay

Withholding

You need to:
- Advise the requester that you are withholding the information (section 44)
- Set out the relevant withholding ground/s (sections 27-29)
- Advise the requester that they can ask the Office of the Privacy Commissioner to review this decision

Figure 11 - Access flowchart
Timeframes for response

There are reasonable timeframes within which an agency must respond to a request. The request may be for access or for correction.

<table>
<thead>
<tr>
<th>Request Type</th>
<th>Time Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response or notification of extension</td>
<td>20 working days</td>
</tr>
<tr>
<td>Transfer</td>
<td>10 working days</td>
</tr>
</tbody>
</table>

Table 5 - Response timeframes

Charging

A public sector agency may not impose a charge for responding to an access request. Private sector agencies may impose a reasonable charge for making the information available. What will amount to a reasonable charge will depend on the circumstances. The OPC considers that the Ministry of Justice Guidelines for Official Information Act 1982 Requests provide a useful starting point.

Under those guidelines, the first hour of labour should be free and an agency may charge $38 for every half hour after that. The first 20 pages of photocopying are free, but the agency can charge 20c per page after that. Another way of working out what a reasonable charge might be would be to obtain a quote from a local copy centre.

Also keep in mind that you can always suggest alternative ways of providing information when responding to a request. For example, an individual may be just as happy to receive their information on a CD or USB (memory) stick for a minimal charge, rather than paying a large amount to have their file photocopied.

You can never charge for any costs involved in deciding whether to make information available, for instance, the cost of retrieving information from archives or for the time taken to reach a decision.
Key point

Public sector agencies **may not** charge for information.

Private sector agencies may make a **reasonable charge** for costs involved in providing the information, but not for the costs involved in making a decision.
Some withholding grounds

The right to access your personal information is a broad right. There are very few situations where it may be legally withheld. These are called **withholding grounds** in the Act, and are discussed below.

An important point to note here is that when you decide to withhold any information you must inform the individual of their right to have that decision reviewed by the Privacy Commissioner. You should also take reasonable steps to keep a record of what information you have withheld and why, and make sure that you retain the information for a reasonable length of time to allow the individual to have the decision reviewed if they want to.

Table 6 shows a limited list of the reasons that an agency may legally not give out personal information.

| Grounds to withhold information from an individual; sections 27-29 of the Privacy Act |
|----------------------------------------|-------------------------------------------------|
| **Section**                           | **Title**                                       |
| Section 27(1)(c)                      | prejudice maintenance of law                   |
| Section 27(1)(d)                      | endanger safety                                |
| Section 29(1)(a)                      | unwarranted disclosure                          |
| Section 29(1)(b)                      | evaluative material, defined in section 29(3)   |
| Section 29(2)                         | not readily retrievable / cannot be found / does not exist |

Table 6 - Withholding grounds under the Privacy Act
If it may prejudice maintenance of the law

Under section 27(1)(c), an agency may withhold information if its disclosure would be likely to prejudice the maintenance of the law, including the prevention, investigation or detection of offences. The Police and other agencies with a law enforcement function often use section 27(1)(c) as a reason not to release information. It is generally expected that at the conclusion of the investigation the information will be released.

However, in limited circumstances some information may continue to be withheld under this section after an investigation has ended. For example, this may be to protect an informant’s identity and to protect investigative technique (how the information was obtained), etc.

Case note 94010 [2007] NZ PrivCmr 6 - beneficiary aggrieved at being denied details of allegations

A female beneficiary requested details of an allegation made against her that would impact on her benefit. She wanted to know the date and time the allegation was made, as well as the name and gender of the person who made the allegation. The Ministry of Social Development provided her with the investigation file but refused to disclose details of the informant. The woman complained to the Privacy Commission. Her complaint was not upheld as the OPC was satisfied the Ministry had a proper basis to withhold this information under section 27(1)(c).

If it may endanger the safety of any individual

Under section 27(1)(d), an agency may withhold information if the disclosure would be likely to endanger the safety of any individual. This means that their physical safety could be compromised (i.e., they would be at risk of harm). If you seek to withhold information on these grounds you must be sure that there is a ‘serious or real and substantial risk, or a risk that may well eventuate’.
If disclosure is unwarranted

Section 29(1)(a) provides a withholding ground where the release of the information would involve the unwarranted disclosure of the affairs of another individual. This section is relevant in cases where the information at hand relates to more than one person and is designed to protect the privacy of other individuals. It is used in cases where, given the circumstances, disclosing the information would be an unwarranted disclosure of another individual’s personal information.

Determining what would be unwarranted involves a balancing exercise between the interests of the individuals involved.

In the past the Commissioner has seen the following factors as relevant:

1. the purpose for which the information was supplied or held
2. the purpose for which the information is requested, and
3. the requester’s prior knowledge

If the information is confidentially supplied evaluative material

Section 29(1)(b) allows an agency to withhold evaluative material where that information has been supplied under an express or implied promise of confidentiality and where disclosing that information would breach that promise. The term ‘evaluative material’ is limited in the Privacy Act to certain types of information including, for instance, job references and information used to make decisions about scholarships and insurance claims.

In order for an agency to be able to rely on section 29(1)(b), they must meet a three part test:

1. The information in question must have been compiled solely for one of the purposes set out under section 29(3); and
2. The information must have been provided with an express or implied promise of confidentiality, and
3. The disclosure of that information would breach that promise.
If it may prejudice physical or mental health

Section 29(1)(c) allows information to be withheld if the agency is satisfied that disclosure would be likely to prejudice the physical or mental health of the individual (the requester). The agency seeking to rely on this ground must consult the requester’s medical practitioner if possible. The medical practitioner does not have to be a doctor (for example, they could be a counsellor or therapist) but they must be someone with an ethical obligation to the requester.

The agency is not obliged to accept the views of the medical practitioner, but must take them into consideration along with other evidence before making a decision. The information requested must relate to the physical and mental health of the requester and the agency must be satisfied that the information in question would prejudice the requester’s health. This is rarely supported because of the requirement for a direct causal link between the information and harm.

If the information is not readily retrievable, does not exist or cannot be found

If the information does not exist or cannot be found then the agency should rely on section 29(2)(b). However, before they rely on this section, they must undertake a reasonable search. The agency also needs to consider that if they are unable to find personal information that they should hold, this may raise issues under principle 5.
1. Follow the directions of your facilitator to form pairs or small groups.
2. Complete Table 7 as directed by your facilitator.

<table>
<thead>
<tr>
<th>Grounds to withhold information from an individual</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>27(1)(c) - prejudice maintenance of law</td>
<td></td>
</tr>
<tr>
<td>27(1)(d) - endanger safety</td>
<td></td>
</tr>
<tr>
<td>29(1)(a) - unwarranted disclosure</td>
<td></td>
</tr>
<tr>
<td>29(1)(b) - evaluative material, defined in section 29(3)</td>
<td></td>
</tr>
<tr>
<td>29(2) - not readily retrievable / cannot be found / does not exist</td>
<td></td>
</tr>
</tbody>
</table>

Table 7 - Examples of withholding grounds
3. Use the space provided to write any notes or questions.
Principle 7 - correction

Key point

Principle 7

People have a right to ask an agency to correct information about themselves if they think the information is wrong.

If the agency does not want to correct the information, it does not usually have to. But if it does not correct the information, it must give the person the opportunity to add their views about what the correct information is.

Principle 7 provides individuals with the right to request correction of information. When an agency receives a request for correction and it does not want to make that correction, it must inform the individual of three things:

1. the reason for the refusal
2. the individual’s right to request that a statement of correction be attached to the disputed information, and
3. the individual’s right to complain to the Privacy Commissioner

The Act does not say what form a reason for refusal must take. However, there is an obligation under principle 7, section 2 to ensure that information is correct. Therefore, the agency may state that the information was the opinion held at the time the information was compiled.

If the agency makes the requested correction or attaches a statement of correction, it is obliged to take two steps:

1. inform any agency which has received the information of any changes made, and
2. ensure that the statement will be read in conjunction with the disputed information

A possibility that you might like to consider, especially where the disputed information is historic, is to separate the disputed information from the file and leave a note in the file as to its existence.
The way your agency must go about responding to correction requests is set out in the Act. The Act calls these procedural provisions and they are the same under principles 6 and 7. The procedural provisions state the following:

1. The agency has an obligation to assist the person making the request (section 38).
2. The agency must inform the individual of its decision on the request within 20 working days of receiving the request (section 40).

Key point

If an agency receives information from other agencies it should attempt to verify the accuracy of the information where possible (this becomes important under principle 8 - accuracy).

Individuals have a right to request correction; or have a statement of correction added.

Agency must either:

- make the change
- attach statement

inform the individual and any recipients of the information

Figure 12 - Individual rights to have information corrected
Correction example

An employee has been accused of sexual harassment by another staff member. The allegations could not be substantiated. The employee now asks that the information be deleted from their personnel file. In the circumstances the organisation wants to retain the information.

Self-check activity

Reflection

Use the space provided to create a mind map of the concepts you have learnt so far about the correction of personal information.
Principle 8 - accuracy

Key point

Principle 8

Before using personal information, an agency must take reasonable steps to ensure it is:

• accurate
• up-to-date
• complete
• relevant
• not misleading

What is reasonable will depend on where the information was obtained and when it was obtained. What is reasonable will also depend on the proposed use. This can be particularly important where information has been obtained from a source other than the person concerned. It may be sensible to verify that information with the person concerned.
1. Use the space provided to write any notes or questions.
An ACC claimant’s attendant care and home help compensation was cancelled after an assessment carried out on behalf the ACC. The claimant was almost completely disabled. There was no likelihood of recovery for the claimant.

During the course of the investigation it became apparent that the assessor had mistakenly attached the wrong assessment to the claimant in which the assessor stated that the claimant enjoyed hanging out the washing and doing the ironing and housework.

The Commissioner found ACC in breach of rule 8. The Commissioner considered that it would have been reasonable in the circumstances to check the assessment with information already held about the complainant. It would also have been reasonable to give the claimant an opportunity to comment on the report because the ACC was considering taking adverse action against him.

**Case note 17749: accuracy example**

**Key question**

*What does accuracy mean?*

When the OPC reviews a principle 8 (accuracy) complaint, the review focuses not on the quality of the decision-making, but on whether or not the agency followed a correct process.
Principle 9 - retention

Key point

Principle 9

Agencies must not keep personal information for too long. They can only keep it for as long as is necessary to carry out the purpose for which the agency obtained the information in the first place.

There is no minimum retention period under the Privacy Act, so if you no longer need it, dispose of it (in a secure way of course!).

Principle 9 requires that agencies do not retain personal information for longer than is required for the purposes for which that information may be lawfully be used. This links with, and provides support to other principles. It discourages agencies from continuing to hold personal information that is no longer needed.

A privacy risk exists where information is retained, because:

- the information may become out of date and therefore should not be used (principle 8)
- the accumulation of information creates a risk that it will be used without regard to the purpose for which it was collected or obtained (principle 10)
- the retention (holding on to) of information increases the risk that it will be inadvertently disclosed (principles 5 and 11)

Figure 13 - It is important to have a policy on how long information will be kept
Retention times and legal obligations

When personal information is no longer required, it can be returned, destroyed or transferred. There are rules around how each should be done. Agencies should have a policy around how to handle personal information when it is no longer needed.

There are several issues that an agency must consider when developing a retention policy:

- Should information be retained (kept) at all (keep in mind that there may be other laws which require you to keep information)?
- If so, for how long?
- How should any information that is no longer required be disposed of? (principle 5)

Other considerations are as follows:

- How long should an employer retain the employment applications of unsuccessful applicants?
- What should be done with the CVs?
- For how long should enrolment information be retained?
- How often are audits conducted to review information?
Case note 243548 (2013) NZ PrivCmr 3: recruitment agency fails to remove all personal information from an old online profile

This complaint came from a former client of the recruitment company, which had created an online profile on his behalf (containing his name, photograph, physical description, qualifications and personal interests).

Once the man ceased to be a client of the agency, he asked for his profile to be removed. The agency removed his name and photo from the online profile, and removed the link to his profile from its website. However, the man later ‘googled’ his name and the edited profile was the first result.

We were satisfied the profile could still be considered to be the man’s personal information (due to the detail of information still on the page, and because Google still linked it to his name). We contacted the agency to raise concerns that it still was making this man’s information available online despite the fact he was no longer a client.

The agency accepted our concerns and completely removed the profile from its website. This action resolved the man’s complaint.
### Self-check activity

1. Complete Table 8 with examples from your agency.
2. Talk to your supervisor or a more experienced workmate where applicable.

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>What are some examples of information held by your agency?</td>
<td></td>
</tr>
<tr>
<td>How long do you hold on to this information?</td>
<td></td>
</tr>
<tr>
<td>Why do you keep it for this long? For example, is it necessary in order to comply with legal obligations or is it your agency’s policy?</td>
<td></td>
</tr>
<tr>
<td>What happens to information you no longer need to retain?</td>
<td></td>
</tr>
<tr>
<td>How often are audits conducted to review information?</td>
<td></td>
</tr>
</tbody>
</table>

Table 8 - Managing data at your agency
Principle 10 - use

Key point

Principle 10

Agencies must use personal information for the same purposes for which they obtained that information.

Other uses are occasionally permitted (for example, where this is necessary to enforce the law, or where the use is directly related to the purpose for which the agency obtained the information).

The key concept of principle 10 is that personal information obtained for one purpose must not be used for another purpose unless the agency believes, on reasonable grounds, that an exception applies. Examples of exceptions are where:

- the other use was authorised by the individual or their representative, or
- the other purpose is directly related to the purpose for which the information was originally collected

Principle 10 is similar to principle 11 - disclosure. Both principles 10 and 11 limit the use and disclosure of information to the purpose for which it was collected or obtained.
Some exceptions to principle 10

Again, non-compliance is permissible in certain circumstances where the agency believes on reasonable grounds that:

- another use is authorised by the individual concerned (section 10(b))
- the other use is directly related to the purpose for which the information was collected (section 10(e))

The agency can use the information for purposes other than the purpose for which it was collected if:

- this is necessary to avoid prejudice to maintenance of the law or the conduct of proceedings before a court or tribunal (section 10(c)(i) and (iv))
- the information is used without identifiers (section 10(f)(i)), or for statistics or research (section 10(f)(ii))
- the information is originally sourced from a publicly available publication and, given the circumstances, it would not be unfair or unreasonable to use that information (section 10(a))

These are not the only exceptions, but cover the most common examples. Questions for you to consider before using personal information you have obtained for another use include:

- What was the purpose of collection?
- Was the individual made aware of that purpose?
1. Follow the directions of the facilitator to complete the activity.
2. Use the space provided to write any notes or questions.
Principle 11 - disclosure

Key point

Principle 11

Agencies must not disclose personal information unless an exception applies. One example is where another law requires them to disclose the information. An agency can disclose information if it reasonably believes, for example, that:

- disclosure is one of the purposes for which the agency obtained the information
- disclosure is necessary to uphold or enforce the law
- disclosure is necessary for court proceedings
- the person concerned authorised the disclosure
- the information is going to be used in a form that does not identify the person concerned

Disclosure of personal information can become an issue in cases where you have been asked for information about an individual by a third party, or in any other case where you want to disclose information about an individual.

Principle 11 provides that an agency must not disclose personal information unless it believes, on reasonable grounds, that an exception applies. The exceptions discussed below are not the only ones, but cover the most common examples.

It is important to note here that disclosure is discretionary - this means that it is the choice of the agency (even if an exception applies). Also remember that if you do disclose information, you should take care to avoid 'over-disclosure' by only disclosing the necessary information.

Also keep in mind that there may be cases where you are required to disclose personal information, for example, if Police obtain a search warrant or if a court has ordered discovery. Because you are required to disclose this information under another law, this overrides principle 11 (see the discussion on section 7 for further information).
Some exceptions to principle 11

The exceptions are similar to those of principle 10. Therefore, for similar reasons, it is extremely important in the first instance that you know your purpose for collecting information and how the information will be used.

An agency must not disclose personal information, unless it believes on reasonable grounds that:

- disclosure is one of the purposes, or a directly-related purpose, for which the information was obtained. (This exception is the most important, and links to principle 3 requiring the individual to be told of any anticipated disclosures.) (section 11(a))
- disclosure is to the individual or authorised by the individual (section 11(c) and (d))
- the individual is not identified (section 11(h) and (i))
- disclosure is necessary to avoid prejudice to the maintenance of the law or the conduct of proceedings before a court or tribunal (section 11(e)(i) and (iv))
- disclosure is necessary to prevent or lessen a serious threat to public health or safety or the life or health of the individual concerned (section 11(f))

In order to decide whether something is a 'serious threat' you need to consider the following questions:

- How likely is it to happen?
- How severe would the consequences be if it did happen?
- When might it happen?

Key point

Safety trumps privacy; if you have concerns that an individual may hurt themselves or others, tell someone who can do something about it (e.g., the Police).
1. Follow the directions of the facilitator to complete this activity.
The flowchart in Figure 14 sets out the steps that must be followed when making a decision about whether to disclose personal information (either because you’ve received a request from a third party, or because you want to).

**DISCLOSING PERSONAL INFORMATION (‘PI’) UNDER THE PRIVACY ACT (THE ‘ACT’)**

- **When you have received a request for PI from anyone other than the individual concerned or their representative**
  - **Are you required to release the PI?**
    - In some cases you may not have a choice about providing requested information, e.g. if Police produce a search warrant or if the request is under section 17 of the Tax Administration Act.
  - **Yes**
  - **No**

- **Disclosure of PI when you have not received a request**
  - **Are you required to release the PI under another piece of law?**
    - Some laws place agencies under an obligation to report certain information, e.g. section 18 of the Land Transport Act 1998.
  - **Yes**
  - **No**

- **Where another law specifically requires disclosure, this overrides the ACT. You can disclose the PI.**
  - **Yes**
  - **No**

- **Are you allowed to release the PI under another law?**
  - In some cases you have the discretion to disclose information, but only if you have received a request first, e.g. the Official Information Act 1982 or section 59 of the Housing Restructuring and Tenancy Matters Act 1992 (HNZC).
  - **Yes**
  - **No**

- **Is there another law which allows you to disclose this information?**
  - Some laws permit disclosure in specific circumstances or for specific reasons, e.g. sections 15-16 of the Children, Young Persons and Their Families Act 1989 or the Protected Disclosures Act 2000.
  - **Yes**
  - **No**

- **If you want to disclose this information, you may do so.**
  - **Yes**
  - **No**

- **Does an exception under principle 11 apply in the circumstances?**
  - Some exceptions allowing for disclosure under rule 11:
    - Where disclosure is one of the purposes which you collected the information for, or disclosure is directly related (principle 11(a)).
    - If the individual consents to disclosure (principle 11(d)).
    - If the information was originally obtained from a publicly available publication (principle 11(b)).
    - Disclosure is necessary to avoid prejudice to the maintenance of the law, or for court or tribunal proceedings (principle 11(e)).
    - Disclosure is necessary to prevent or lessen a serious threat (having regard to likelihood, severity and imminence) (principle 11(f)).
  - **Yes**
  - **No**

- **You can disclose the information, if you want to.**
  - **Yes**
  - **No**

- **You should also make a note of what PI was disclosed and your reasons for disclosure.**

If you have any questions or concerns about disclosing personal information, feel free to contact our enquiries team on 0800 803 909 or enquiries@privacy.org.nz for guidance.

**Figure 14 - Disclosure flowchart**
1. Work in pairs or small groups as directed by your facilitator.
2. Follow the directions of the facilitator to complete Table 9.

<table>
<thead>
<tr>
<th>Disclosure questions</th>
<th>Yes / No</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Police if they are investigating a case</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A spouse requesting bank account details about their partner</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A friend of the individual who wants current contact details</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A lawyer acting for another party in court proceedings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Someone who claims they are acting on behalf of the individual</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 9 - Disclosure questions
Group activity

3. Use the space provided to write any notes or questions.
Principle 12 - unique identifiers

Key point

Principle 12

Some agencies give people a **unique identifier** instead of using their name. Examples are a driver’s licence number, a student ID number or an IRD number.

An agency cannot use the unique identifier given to a person by another agency. People are not required to disclose their unique identifier unless this is one of the purposes for which the unique identifier was set up (or directly related to those purposes).

A unique identifier is an identifier that is assigned to an individual by an agency for the purpose of its operations to uniquely identify the individual in relation to that agency.

Principle 12 restricts the use of unique identifiers. An agency may only assign a unique identifier if:

- this is necessary to enable it to carry out its functions
- the person’s identity is clearly established

Principle 12 is written this way to lessen the risk that a ‘de facto universal identifier’ will emerge (consider the situation in America where the Social Security Number (along with name and date of birth) is considered proof of identity). If the same number is used across all agencies, there are risks that people’s information may be compromised and identity theft will be easier and do more damage. If fraud and damage of information occurs, this will affect individual privacy.
There are four parts to principle 12:

1. Agencies are not to assign unique identifiers unless it is necessary to enable them to carry out their functions efficiently.

2. Agencies cannot assign a unique identifier that has been assigned by another agency. E.g., The Bank cannot use your IRD number as your customer number.

3. When an agency assigns a unique identifier, it must take reasonable steps to ensure that unique identifiers are only assigned to individuals whose identity is clearly established.

4. You cannot require an individual to disclose their unique identifier, unless the disclosure is one of the purposes in connection with which that unique identifier was assigned (or a directly related purpose). For example, Police can ask you to provide your driver’s licence (which includes a unique identifier) when they are carrying out a traffic stop, even though the driver’s licence is issued by another agency (NZTA).

Key point

An agency must not use identifier assigned by another agency. (The NHI number is an exception).
Interference with privacy

When an individual complains to the OPC that their privacy has been breached, the legal test to be met is whether there has been an *interference with privacy* (section 66).

The test will be slightly different depending on the type of breach the individual is complaining about.

For a complaint about access to or correction of personal information, simply breaching the Privacy Act will result in an interference with privacy. For all other complaints, an interference with privacy will require that there has been a breach of the Act and that the breach resulted in harm of the type required under the Act.

Breach

Key point

Access and correction complaints are complaints about an information privacy request. Information privacy requests are also called ‘section 6 and 7 requests’ or ‘Access and correction requests’.

All complaints that do not come under principles 6 and 7 are called ‘general interference complaints’.

A breach is defined as something that breaks one of the principles of the Privacy Act. The breach may be of:

- one of the Privacy Act’s 12 privacy principles, which govern how people and organisations collect, use, disclose, store and give access to personal information
- a Privacy Code of Practice that governs a specific area, such as the Health Information Privacy Code
- the privacy provisions relating to data matching between government agencies.

With the rights of access and correction, there will be deemed interference if there was no proper basis for your decision. This is because principles 6 and 7 are rights. You have an obligation to perform as per the principles of the Act. No adverse consequence is required to flow from a breach of principles 6 and 7.
Complaints about information privacy requests

Key point

Requests for access to or correction of personal information under the Act are referred to as information privacy requests.

Because the rights of access and correction are such important rights, they are treated slightly differently from the rest of the Act in terms of complaints (section 66(2)).

This means that for information privacy request complaints there will be an interference with privacy where there is no proper basis for a decision on a request, including:

- a refusal to make information available
- a failure to comply with procedural provisions
- the manner in which information is made available
- an undue delay in making information available
- imposing conditions on the use of information made available
- a failure to respond within 20 working days
- charging more than allowed (or at all if a public sector company)
- a refusal to correct or attach a statement of correction if requested to do so

In the Office it is called an automatic interference if you have no proper basis for your decision or you failed to adhere to the procedural provisions. For this reason it is very important for your agency to have a clear process for responding to information privacy requests.
All other complaints

Key point

For all other complaints about breaches under the Privacy Act (breaches of principles 1-5 and 8-12) the test for an interference is breach and harm.

According to the Act, an ‘interference with an individual’s privacy’ can be defined as a breach of a privacy principle or health code rule and an adverse consequence (section 66(1) of the Privacy Act).

Generally there will be an interference with privacy if:

1. an action breaches a principle, and
2. there are adverse consequences

This is the case for principles 1-5 and 8-12. Harm must flow from the breach. As set out above, this does not apply to access and correction requests (principles 6 and 7).

Adverse consequence

The adverse consequences (what is meant by ‘harm’ as the result of a breach of the Act) are found in section 66(1)(b) of the Privacy Act.

To be considered ‘adverse consequences’, the breach must have led to (or may lead to):

- financial loss or other injury
- an adverse effect on a right, benefit, privilege, obligation or interests
- significant humiliation, significant loss of dignity, or significant injury to the feelings of the individual.
An interference with an individual’s privacy =

for information privacy request complaints (principles 6 and 7)
breach = automatic interference

for all other complaints (principles 1-5, 8-12)
breach + adverse consequence = interference

The harm must be significant. The interference is important because if the OPC finds an interference with privacy they can refer the matter to the Human Rights Review Tribunal.
1. Work in groups as directed by your facilitator.
2. Follow the directions of the facilitator to complete Table 10.
3. Justify your answers. Think about the following questions:
   • What principles (if any) have been breached?
   • What harm has been caused?
   • Use the space provided to write any notes or questions.
## Interference questions

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Has there been an interference with privacy? (Explain your answers.)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fred</strong></td>
<td></td>
</tr>
<tr>
<td>Fred wrote and asked his former employer for a copy of his personnel file. 32 days later he still had not heard anything from the employer about his request. On the 33rd day he received a letter from the employer stating that Fred could come and look at his file, but only if the employer is present.</td>
<td></td>
</tr>
<tr>
<td><strong>Tim</strong></td>
<td></td>
</tr>
<tr>
<td>Tim’s personnel file is accidentally left in the tea room where he works.</td>
<td></td>
</tr>
<tr>
<td>What if?</td>
<td></td>
</tr>
<tr>
<td>a) Before any one looks at his file the HR manager discovers it and locks it away.</td>
<td></td>
</tr>
<tr>
<td>b) The file is left in the tea room overnight. During that period other employees read the file and make copies of warnings on the file, which they stick to the staff notice board.</td>
<td></td>
</tr>
<tr>
<td><strong>Mary</strong></td>
<td></td>
</tr>
<tr>
<td>Mary alleges that her husband, Jack, telephoned her bank to obtain the balance of their joint cheque account. Jack was also given the balances of Mary’s personal accounts. Jack had no idea that these accounts existed and was angry that Mary had kept this information from him. Jack had a violent temper and assaulted Mary.</td>
<td></td>
</tr>
</tbody>
</table>

Table 10 - Interference questions
4. Use the space provided to write any notes or questions.
The complaint intake process is as follows:

1. An individual makes a written complaint
   The complaint intake process begins with a letter or email from an individual alleging an interference with their privacy has occurred.

2. OPC makes an initial assessment
   Complaints are initially assessed to determine whether the Privacy Commissioner has jurisdiction to investigate the complaint.

3. The OPC may need to refer the complaint
   The Commissioner only has jurisdiction to investigate a complaint if it concerns personal information. It may be necessary to refer the complaint to the Office of the Ombudsman if the complaint involves official information. Or to other agencies if it is more appropriate - for example, the Health and Disability Commissioner or the Banking Ombudsman.

4. The OPC may decline to investigate
   If the issue complained about has already been canvassed and no breach has been found or the complainant has not suffered any adverse consequences, the Commissioner may decline to investigate the matter. The Commissioner may also decline to investigate if the matter complained about occurred too long ago for an investigation to be desirable or practicable, or if the person making the complaint does not have sufficient interest in the subject of the complaint (e.g., they are not complaining about their own information).

5. The Investigations Team assesses the complaint
   If the Office does have jurisdiction and new issues are raised, then the file is looked by the Investigations Team.

This complaint intake process is simplified in Figure 15.
Complaint Intake Process

Complaint alleges breach of Privacy Act or Code

Does the Privacy Commissioner have jurisdiction?

Yes

Complaint considered by Investigations Team and assigned to an Investigator

No

Complaint transferred or declined

Figure 15 - OPC complaint intake process
Complaints process

When a complaint is investigated by the OPC, it follows the steps detailed below.

Investigation

When the complaint is assigned to an investigating officer, they will begin by assessing the complaint and deciding whether they need further information. They may call, email or write to the individual to request more detail.

Notification

Once the investigator considers that they have sufficient information, they will then notify the agency against which the complaint has been made and invite them to comment. The investigator may decide that it would be helpful to meet with one or both of the parties to the complaint. If necessary the investigator may call a compulsory conference, which both sides are required to attend for the purposes of clarifying the complaint and attempting to reach a settlement.

Settlement is encouraged

One of the main roles of the OPC is to assist in facilitating the settlement of complaints. As such, throughout the investigation the OPC will consider whether settlement is possible and will encourage the parties to settle where appropriate.

Settlements will differ from case to case may include an apology, an assurance against repeating the action which led to the complaint or a change of process, or compensation. However, the parties are free to be as creative as they like when trying to reach a settlement, so the OPC has seen some fairly inventive settlements, including things like gift vouchers, flowers and fruit!

If no settlement is reached

If the parties do not settle - a preliminary view is formed. This is not the final decision, but gives an indication to the individual and / or the agency of how the decision may go. This goes to the party the OPC is finding against (i.e. the person for whom the decision did not go their way). Sometimes it may be a split primary view, with some issues going to one party and some to the other. The parties have a right of reply.

After parties have responded to a preliminary view, a final legal view will be formed on the matter.

If a complaint with substance (i.e. there has been an interference) is still not settled satisfactorily, the Commissioner has the discretion to refer the complaint to the Director of Human Rights Proceedings - who may decide to bring proceedings in the Human Rights Review Tribunal (HRRT).
If the OPC do not refer

If the OPC do not refer, the complainant may take proceedings before the HRRT themselves. The difference is that if the OPC refers the complaint, it will be liable for any costs incurred if the case is not successful. However, if the individual takes the case themselves and is unsuccessful, they will have to make a contribution to the costs incurred by the other party.

Reasons why the OPC may, or may not, refer include:
- a reasonable settlement was offered and refused
- the availability of proper alternatives to the HRRT
- the seriousness of the complaint
- the behaviour of the respondent agency
- evidential insufficiency
- precedent setting

Human Rights Review Tribunal powers

The HRRT has the same powers as a District Court and can award various remedies including damages of up to $200K. The individual or agency can appeal the HRRT decision to the High Court, then the Court of Appeals, all the way to the Supreme Court.

Damages

To date the most awarded for a breach of the Privacy Act in the HRRT is $40K. However, larger settlements than this have been reached through the OPC.

The full complaints process is simplified in Figure 16.
Complaints Process

Key point

For further information www.nzlii.org is a very useful website for previous Tribunal decisions.
Group activity

1. Follow the directions of your facilitator to form groups.
2. Complete the task as directed by your facilitator.
3. Use the space provided to write any notes or questions.
## Glossary

This list shows some of the words that have been used, and what they mean in this workbook.

<table>
<thead>
<tr>
<th>Word</th>
<th>What it means in this workbook</th>
</tr>
</thead>
<tbody>
<tr>
<td>assessment</td>
<td>Finding out about what has happened and what needs to be done.</td>
</tr>
<tr>
<td>authorised</td>
<td>Allowed; given permission; given the okay.</td>
</tr>
<tr>
<td>breach</td>
<td>The act of breaking a law or agreement.</td>
</tr>
<tr>
<td>data</td>
<td>Stored information.</td>
</tr>
<tr>
<td>Codes of Practice</td>
<td>Rules created by the Privacy Commissioner to regulate how certain industries deal with personal information. These codes form part of the Privacy Act.</td>
</tr>
<tr>
<td>consequences</td>
<td>What will happen as the result of an action.</td>
</tr>
<tr>
<td>contain</td>
<td>Hold in; prevent (an event) from happening or (effects) from spreading. For example, you could contain a data breach by closing down a website.</td>
</tr>
<tr>
<td>disclose</td>
<td>Tell (to another person of agency).</td>
</tr>
<tr>
<td>employee</td>
<td>A person who is employed or contracted by an agency.</td>
</tr>
<tr>
<td>enquiries</td>
<td>Questions or queries.</td>
</tr>
<tr>
<td>grounds</td>
<td>Good (legal) reasons.</td>
</tr>
<tr>
<td>Health Industry Privacy Code (HIPC)</td>
<td>The privacy laws that apply to the health industry.</td>
</tr>
<tr>
<td>incident</td>
<td>A thing that has happened.</td>
</tr>
<tr>
<td>individual(s)</td>
<td>A person or people.</td>
</tr>
<tr>
<td>interference</td>
<td>A breach of one or more of privacy principles 1-5 or 8-12 and an adverse consequence; or a breach of principles 6 or 7.</td>
</tr>
<tr>
<td>Word</td>
<td>What it means in this workbook</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>investigate</td>
<td>Find out what is happening or has happened.</td>
</tr>
<tr>
<td>jurisdiction</td>
<td>The power and authority to carry out an investigation.</td>
</tr>
<tr>
<td>mandatory</td>
<td>Must be done; is required to be done, e.g., by law.</td>
</tr>
<tr>
<td>notification</td>
<td>Telling other people or the authorities.</td>
</tr>
<tr>
<td>notify</td>
<td>Tell.</td>
</tr>
<tr>
<td>obligation</td>
<td>Requirement.</td>
</tr>
<tr>
<td>occur</td>
<td>Happen.</td>
</tr>
<tr>
<td>practice</td>
<td>The usual way of doing something.</td>
</tr>
<tr>
<td>procedural provisions</td>
<td>What needs to be done, and how.</td>
</tr>
<tr>
<td>purpose</td>
<td>The reason for doing something.</td>
</tr>
<tr>
<td>retain</td>
<td>Keep.</td>
</tr>
<tr>
<td>retention</td>
<td>Keeping or holding on to.</td>
</tr>
<tr>
<td>sensitive</td>
<td>High risk; could be harmful to people or the organisation.</td>
</tr>
<tr>
<td>significance</td>
<td>Importance.</td>
</tr>
<tr>
<td>simultaneously</td>
<td>At the same time.</td>
</tr>
<tr>
<td>source</td>
<td>Where something comes from.</td>
</tr>
<tr>
<td>succession</td>
<td>One after the other.</td>
</tr>
<tr>
<td>third party</td>
<td>Another person or agency (i.e. not you or the person directly concerned).</td>
</tr>
<tr>
<td>transferred</td>
<td>Sent somewhere else.</td>
</tr>
<tr>
<td>unauthorised</td>
<td>Not allowed.</td>
</tr>
<tr>
<td>voluntary</td>
<td>Optional; open to choice.</td>
</tr>
</tbody>
</table>
Additional resources

Icebreakers and training ideas: http://www.businessballs.com/
Tribunal decisions: www.nzlii.org

How to contact the Office of the Privacy Commissioner

Website: www.privacy.org.nz

PO Box 10-094
The Terrace, Wellington 6143
Fax: (04) 474 7595

Enquiries line (for general enquiries):
0800 803 909 (from 8.30am to 5pm, Monday to Friday)
enquiries@privacy.org.nz

04-474 7590 (Wellington)
09-302 8680 (Auckland)
The Privacy Act principles: quick reference guide

Principle 1 - purpose for collection

Personal information must only be collected when:

- the collection is for a lawful purpose
- the purpose is connected with the functions of the agency, and
- it is necessary to collect the information for that purpose

Principle 2 - source of information

Personal information must usually be collected from the person who the information relates to. But the Privacy Act does allow you to collect information from other people in limited cases, for instance, when:

- the person concerned authorises collection from someone else
- obtaining it from the person concerned would undermine the purpose of the collection
- this is necessary in order for a public sector body to uphold or enforce the law
- this is necessary for the purposes of court or tribunal proceedings

Principle 3 - what to tell an individual

When an agency directly collects personal information, it has to take reasonable steps to make sure that person concerned knows things like:

- why it is being collected
- who will see the information
- whether the person is required to give the information or whether it is voluntary
- what will happen if the information isn’t provided

Again, there are sometimes good reasons for not letting a person know. For example, it could undermine the purpose of the collection, or it is just not possible to tell the person.
Principle 4 - manner of collection

Personal information must not be collected by unlawful means or by means that are unfair under the circumstances or unreasonably intrusive.

Principle 5 - storage and security

It is impossible to prevent all mistakes. But any agency must ensure that it takes reasonable steps to prevent the loss, misuse or disclosure of personal information.

Principle 6 - access

People have the right to ask for access to personal information about themselves.

Agencies can refuse to give access in some limited situations, for instance, where giving the information would:

- endanger a person’s safety
- prevent the detection and investigation of criminal offences
- involve an unwarranted breach of someone else’s privacy

Principle 7 - correction

People have a right to ask an agency to correct information about themselves if they think the information is wrong.

If the agency does not want to correct the information, it does not usually have to. But if it does not correct the information, it must give the person the opportunity to add their views about what the correct information is.

Principle 8 - accuracy

Before using personal information, an agency must take reasonable steps to ensure it is:

- accurate
- up-to-date
- complete
- relevant
- not misleading
Principle 9 - retention

Agencies must not keep personal information for too long. They can only keep it for as long as is necessary to carry out the purpose for which the agency obtained the information in the first place.

There is no minimum retention period under the Privacy Act, so if you no longer need it, dispose of it (in a secure way of course!).

Principle 10 - use

Agencies must use personal information for the same purposes for which they obtained that information.

Other uses are occasionally permitted (for example, where this is necessary to enforce the law, or where the use is directly related to the purpose for which the agency obtained the information).

Principle 11 - disclosure

Agencies must not disclose personal information unless an exception applies. One example is where another law requires them to disclose the information. An agency can disclose information if it reasonably believes, for example, that:

- disclosure is one of the purposes for which the agency obtained the information
- disclosure is necessary to uphold or enforce the law
- disclosure is necessary for court proceedings
- the person concerned authorised the disclosure
- the information is going to be used in a form that does not identify the person concerned

Principle 12 - unique identifiers

Some agencies give people a unique identifier instead of using their name. Examples are a driver’s license number, a student ID number or an IRD number.

An agency cannot use the unique identifier given to a person by another agency. People are not required to disclose their unique identifier unless this is one of the purposes for which the unique identifier was set up (or directly related to those purposes).