

A quick tour of the privacy principles

The Privacy Act 2020 has 13 privacy principles that govern how you should collect, handle and use personal information.

Principle 1

You can only collect personal information if it is for a lawful purpose and the information is necessary for that purpose. You should not require identifying information if it is not necessary for your purpose.

Principle 2

You should generally collect personal information directly from the person it is about. Because that won't always be possible, you can collect it from other people in certain situations. For instance, if:

- the person concerned gives you permission
- collecting it in another way would not prejudice the person's interests
- collecting the information from the person directly would undermine the purpose of collection
- you are getting it from a publicly available source.

Principle 3

When you collect personal information, you must take reasonable steps to make sure that the person knows:

- why it's being collected
- who will receive it
- whether giving it is compulsory or voluntary
- what will happen if they don't give you the information.

Sometimes there may be good reasons for not letting a person know you are collecting their information – for example, if it would undermine the purpose of the collection, or if it's just not possible to tell them.

Principle 4

You may only collect personal information in ways that are lawful, fair and not unreasonably intrusive. Take particular care when collecting personal information from children and young people.

Principle 5

You must make sure that there are reasonable security safeguards in place to prevent loss, misuse or disclosure of personal information. This includes limits on employee browsing of other people's information.

Principle 6

People have a right to ask you for access to their personal information. In most cases you have to promptly give them their information. Sometimes you may have good reasons to refuse access. For example, if releasing the information could:

- endanger someone's safety
- create a significant likelihood of serious harassment
- prevent the detection or investigation of a crime
- breach someone else's privacy.

Principle 7

A person has a right to ask an organisation or business to correct their information if they think it is wrong. Even if you don't agree that it needs correcting, you must take reasonable steps to attach a statement of correction to the information to show the person's view.

Principle 8

Before using or disclosing personal information, you must take reasonable steps to check it is accurate, complete, relevant, up to date and not misleading.

Principle 9

You must not keep personal information for longer than is necessary.

Principle 10

You can generally only use personal information for the purpose you collected it. You may use it in ways that are directly related to the original purpose, or you may use it another way if the person gives you permission, or in other limited circumstances.

Principle 11

You may only disclose personal information in limited circumstances. For example, if:

- disclosure is one of the purposes for which you got the information
- the person concerned authorised the disclosure
- the information will be used in an anonymous way
- disclosure is necessary to avoid endangering someone's health or safety
- disclosure is necessary to avoid a prejudice to the maintenance of the law.

Principle 12

You can only send personal information to someone overseas if the information will be adequately protected. For example:

- the receiving person is subject to the New Zealand Privacy Act because they do business in New Zealand
- the information is going to a place with comparable privacy safeguards to New Zealand
- the receiving person has agreed to adequately protect the information – through model contract clauses, etc.

If there aren't adequate protections in place, you can only send personal information overseas if the individual concerned gives you express permission, unless the purpose is to uphold or enforce the law or to avoid endangering someone's health or safety.

Principle 13

A unique identifier is a number or code that identifies a person in your dealings with them, such as an IRD or driver's licence number. You can only assign your own unique identifier to individuals where it is necessary for operational functions. Generally, you may not assign the same identifier as used by another organisation. If you assign a unique identifier to people, you must make sure that the risk of misuse (such as identity theft) is minimised.