Privacy Commissioner
Te Mana Matapono Matatapu


# Privacy and CCTV

## A guide to the Privacy Act for businesses, agencies and organisations

Privacy and CCTV
A guide to the Privacy Act for businesses, agencies and organisations

Published by the Office of the Privacy Commissioner
PO Box 10094
Wellington
gen-i Tower
109-111 Featherston Street
Wellington 6143



ISBN 04 478 11730 2

# Table of contents

**Introduction** ..... **3**

**1. Deciding whether CCTV is right for you** ..... **6**

**2 Have a clear plan** ..... **8**

**3 Selecting and positioning cameras** ..... **11**

**4 Make people aware of the CCTV** ..... **13**

**5 Collecting only necessary images** ..... **15**

**6 Using the CCTV images** ..... **16**

**7 Storage and retention of images** ..... **18**

**8 Controlling who can see the images** ..... **20**

**9 Audit and evaluation** ..... **23**

**Appendix A: CCTV checklist for small businesses** ..... **25**

**Appendix B: Privacy Act principles** ..... **26**

# Introduction

In the last decade, CCTV technology has improved enormously and has become cheaper and easier to use. While highly sophisticated systems are still expensive and so, realistically, are only available to public authorities or major businesses, small business owners and even individuals can now install and use basic CCTV systems with ease. The result is that CCTV is now commonplace in New Zealand.

Because CCTV captures images of people, which can be used, stored, manipulated and disseminated, those who operate the systems need to be aware of how to manage privacy issues. Good management of personal information is essential to the effective running of CCTV systems (including ensuring that they are cost-effective). Businesses can only take advantage of the full benefits available from CCTV technology if they manage their system with privacy in mind.

Major organisations more commonly have the resources – and the legal compliance knowledge – to ensure that they address those issues. However, up to now, smaller operators have often been unsure how to find out how to manage their systems.

These guidelines attempt to close that gap. They will assist organisations of all sizes to manage CCTV systems in line with their legal obligations and good personal information handling practice. They aim to:

- deliver simple, practical help to those wishing to set up and operate CCTV, whatever the size of their organisation;
- encourage them to set up CCTV systems in ways that protect the privacy of individuals;
- help them to comply with their legal obligations under the Privacy Act; and
- encourage them to use best privacy practice, including using privacy-enhancing technologies.

If you are a small business or organisation, use the checklist in Appendix A for a quick guide to what you have to do. Then consult the rest of these guidelines, as they explain the points in the checklist.

## What do we mean by “CCTV”?

“CCTV” or “closed circuit television” is a somewhat outdated term, given the changes in the technology. However, it is still the shorthand term that is in most common use, so we have employed it in these guidelines.

When we talk about “CCTV”, we mean camera surveillance systems that capture images of individuals or information relating to individuals.

For example, a CCTV system may be used:

- to track or monitor what an individual (or group of individuals) is doing, for example in a shop or walking down the street;
- to capture information that could be used to investigate a crime;
- to use surveillance as a means of deterring crime.

Some camera surveillance systems involve recording of information and others may involve only real-time viewing of information. Different aspects of these guidelines may apply depending on the type of system involved.

## Who should use these guidelines?

If you are an **"agency"** under the Privacy Act, you should use these guidelines. Nearly every person, organisation or business that collects, holds or uses information about individuals is an "agency". Only bodies such as courts or tribunals, or Parliament, or the news media when they are gathering or publishing news, are exempt from being "agencies".

So if you are in New Zealand and you want to set up and/or operate CCTV, these guidelines are almost certainly for you. They apply equally to the public and private sectors, and to organisations of all sizes.

## Scope of the guidelines

These guidelines do not attempt to cover all aspects of CCTV. For instance, we do not deal with covert CCTV (which is subject to special considerations and, often, special legal rules). Nor do we deal with surveillance systems in the home or other entirely private spaces. Instead, we focus on the majority of CCTV systems – that is, **non-covert CCTV** in **public and semi-public spaces**.

- By **'non-covert'** we mean CCTV that is visible and that the people being monitored know about. For example, individuals can see the CCTV camera or there is a sign informing them about the camera.
- By **'public spaces'** we mean spaces that are completely accessible to the public, such as streets, footpaths and public parks.
- By **'semi-public spaces'** we mean spaces that (even if privately owned) are accessible to the public during opening hours. These include banks, libraries, shops, hospitals, malls, sports centres, educational institutions, taxis, trains or other transport systems, restaurants and so on.

## What privacy issues are covered?

The guidelines reflect the information privacy principles in the Privacy Act. These deal with issues such as:

- being clear about why you are collecting information about people;
- making sure people know about the cameras and their purpose;
- how you use CCTV images;
- whether you disclose CCTV images or information to others (such as the Police);
- how long to keep the images for;
- keeping images safe, and making sure that only authorised people can see them; and
- rights of access to the information by the individual concerned.

So, to a large extent, the guidelines reflect your legal obligations in relation to CCTV. Occasionally, though, they indicate best practice – particularly where good privacy protection will help to enhance your business.

## How to use the guidelines

Each section of the guidelines has three main parts.

- The first part gives a brief outline of how the Privacy Act applies to that particular aspect of CCTV. The relevant principles are in bold for easy reference. That way, if you want more information you can go to Appendix B, which contains the privacy principles, and find the text of the law.
- Second, the guidelines themselves are in a highlighted box and are numbered.
- The third part offers a bit more explanation about each of the guidelines to help you understand how to follow them. It may also include examples relevant to different sectors.

The first two sections of the guidelines will guide you through developing three key documents:

1. **an evaluation** of whether you need CCTV and what form that system might take;
2. **a business plan** which sets out your CCTV strategy; and
3. **a CCTV policy** which outlines how you will operate your system and the rules your staff will abide by when using the system.

For small businesses, this may look a little daunting but in fact these documents need not be onerous to produce, and are well worth the effort. They will help to ensure that you can operate your CCTV system legally, and that it is worth the resources that you are investing in it.

# 1. Deciding whether CCTV is right for you

Before you install CCTV, you need to make an informed decision about whether it is really necessary. This fits in with **principle 1** of the Privacy Act, which says that personal information shall not be collected unless:

- the information is collected for a lawful purpose connected with a function or activity of the agency; and
- the collection of the information is **necessary** for that purpose.

**Principles 10** and **11** also say you may only use and disclose personal information for the purpose that you collected it (except in certain specific circumstances).

So knowing your purpose for collecting personal information is important.

## Guidelines

1.1 Clearly identify what you need CCTV for. This is your **purpose** for using CCTV.

1.2 Carefully consider whether CCTV will actually meet your needs. Identify:

- the existing problem you seek to address;
- whether CCTV could address that problem and, if so, how; and
- whether there are other alternative options available.

1.3 Think about whether it would be useful to consult with people who will be affected. If so, talk to them.

1.4 You should repeat the steps above when expanding existing CCTV systems, and at regular intervals during the life of a CCTV system.

### Guideline 1.1 – Identifying what you need CCTV for

Identifying the purpose of your proposed CCTV system is essential – that is, the reason you want to collect and use personal information. The Privacy Act requires that you have a clearly defined purpose when you collect personal information (and that you only use the information for that purpose). Also, you cannot adequately judge how effective your system is, or whether it is worth the expense and the risk to privacy or trust involved, unless you are clear about why you need it.

There can be many different reasons for using CCTV. For instance:

- it may detect and capture evidence of crime;
- it may actively deter crime; or
- it may allow a quick response to traffic accidents or other emergency situations.

Clearly state the purpose or purposes of your proposed CCTV system. When you do so, make sure you are specific. For instance, if your purpose for using CCTV is to prevent crime, explain the types of crime you seek to prevent.

Being specific about the purpose of the CCTV:

- helps you to comply with the law;
- makes it easier to assess the success of your system later on; and
- helps you to explain why the system is there to your staff, members of the public, or to whoever else will be affected by the cameras.

**Guideline 1.2 – Evaluating the need for CCTV**

This will help you make good decisions about whether CCTV is necessary and, if it is, what type of system is best for you.

Sometimes a negative incident, such as a hold-up in a shop, can result in the shop-owner feeling under pressure to install CCTV. However, it is important to resist a knee-jerk reaction. Instead, weigh up the evidence and decide whether CCTV is really the *right* response to that incident. There may be other options that could address your problem better than CCTV or that could be used alongside CCTV to make it more effective.

- Collect some facts and figures so you can see whether CCTV will fix your problem. For instance, if you are a small business with a shoplifting problem, what exactly is the scale of that problem? Or, if you are a large agency looking at installing CCTV cameras on city streets to address crime, collect statistics on the number and types of crimes in the area and the times they occur. If you do go ahead with CCTV, this will help to determine later on whether the CCTV has had an impact on the problem. If you do not collect this information, you have no way of checking whether the cameras are working, and whether you should continue to invest in them.
- Get some information about whether CCTV is likely to address your problem. For example, there is doubt about how effective CCTV is in preventing violent crimes, but research indicates it can be more effective in deterring property crime such as vehicle theft. Check with your local Chamber of Commerce or industry association – it may have some useful information for you to consult.
- Are there other options that might achieve the same benefits or objectives?
- What effect will it have on people? For instance, will it be stressful for your employees, or put off your customers?
- Are there ways of making it less intrusive?
- How much is it likely to cost – to set it up, to run it and to maintain it?

An evaluation need not be an extensive, time-consuming process. What you should do will depend on the size of the proposed system and the level of impact it is likely to have on people's privacy.

**Guideline 1.3 – Consultation**

If at all possible, as part of your evaluation process, talk to people who will be affected by the CCTV system. For instance, if you have employees who will be filmed by the cameras, you should definitely discuss things with them. Explaining the purpose of the CCTV, and getting your staff on-side will make the system more effective. Also, talking to others can give you excellent information – such as indicating whether CCTV might cause you problems that you had not thought about.

Depending on the size of your system, and the reasons for installing it, it may also be useful to consult with:

- customers and clients;
- public interest groups;
- local community groups;
- other businesses;
- other agencies similar to your own that use CCTV
- security specialists; and
- the Police.

With large-scale evaluation and consultation processes, it is a good idea to appoint a senior manager to be responsible for the project. It might also be appropriate to form a working group with different interests represented.

**Guideline 1.4 – Evaluating the need for expansions of CCTV**

Any time you significantly change your system, do a new evaluation to make sure that you are still managing the privacy issues successfully.

It is also important to keep checking that the CCTV system is achieving the results that you want, so do an evaluation regularly. (See guideline 9.1).

# 2. Have a clear plan

While the evaluation under guideline 1 is aimed at helping you decide *whether* to use CCTV, the business plan is the detailed document you produce *after* you have made a decision to go ahead with CCTV. It guides what you will do from now on.

It is worth spending some time on developing your business plan, though it does not need to be a difficult or costly task. Having good documentation can prevent mistakes later, and can save you a lot of time and money.

## Guidelines

2.1 Develop a business plan for the CCTV system, setting out:

- the purpose of the system;
- the outcome/s that you expect;
- the type of technology and equipment that will be used;
- how the system will be operated; and
- how privacy impacts will be minimised.

2.2 Where appropriate, consult with the community and other key stakeholders on your business plan.

2.3 Appoint a person to be responsible for the operation of the CCTV system.

2.4 Develop a clear policy on how images collected by CCTV will be handled. Make this policy easily accessible (for example, on your website).

2.5 Train staff in your policies and procedures for the CCTV system.

**Guidelines 2.1 and 2.2 – Developing and consulting on a business plan**

In your business plan reiterate the key purpose of the CCTV system to make sure you do not accidentally stray from this as you plan your system.

You can also now add detail around exactly what sort of CCTV system you will install and how it will operate. This planning stage is critical to ensuring you end up with a system that achieves all of your goals and objectives.

The topics you cover in your business plan can include:

- an assessment of what type of equipment will best balance your needs with managing privacy issues (check the rest of these guidelines to identify the privacy issues you need to address);
- detailed information on the start-up and running costs of the CCTV, and any additional resources you will require (for instance a staff member's time);
- proposed location and field of vision of your CCTV system;
- who will operate the CCTV, and who will be responsible for it;
- who will be able to see the images;
- how you will inform the public that CCTV is operating;
- what you intend to do with the CCTV images you obtain; and
- what risks there are and how you will manage them.

As with the initial evaluation you did under guideline 1, it is worth talking about your business plan with people who will be affected.

**Guideline 2.3 – Have a person responsible for the CCTV**

Whatever the size of your organisation, it is important to have someone in charge of the CCTV system who will:

- oversee how it works;
- take responsibility for enquiries from the public;
- deal with any problems or issues; and
- help you develop your policies and train your staff.

It is particularly important to set out clearly who is responsible if the CCTV system is being deployed by two or more agencies in partnership. For example, local councils often work closely with the Police to establish CCTV systems. In these circumstances, it is useful to have an agreement in place at the start that clearly sets out who has responsibility for what. This will minimise risks of miscommunication and mistakes.

**Guideline 2.4 – Develop a CCTV policy**

Privacy and good information handling need to be built in at the very start. It is much harder to incorporate privacy protections later on when the system is already operating. So having policies in place early is a key to the success of the system as a whole.

Your business plan will already have outlined many of the points you need to include in your policy (see guideline 2.1) so writing that policy is likely to be straightforward.

The guidelines throughout this document will offer help and direction for many of the issues you should consider in your policy, so again read the rest of this document before you start writing the policy.

Some of the key areas to include are:

- when the cameras will operate;
- if and how cameras will be monitored;
- how incidents captured by CCTV will be reported or acted on;
- access to, and security of, images;
- who will keep the footage and how long it will be kept;
- securely deleting the footage, and who will do this;
- who the public should contact if they have any enquiries;
- how any complaints will be handled;
- what might happen to a staff member if they breach the policy;
- how you will find out whether your policy is being complied with (eg audit); and
- when other audits and review will take place.

If you have a website, put your policy on it. Since not everyone will have access to your website, though, you should also have hard copies available on request.

Making your policy available for people to look at will help people understand why you have CCTV and how it works. It will also show that you have controls and procedures in place for your use of the cameras, which will minimise the concerns that people might otherwise have.

**Guideline 2.5 – Training staff**

A policy is only effective if it is put into practice. So make sure you:

- train all staff who will be involved in the CCTV operations, so they know exactly what to do;
- provide refresher training for those staff periodically, so they and you can continue to be confident that things are operating smoothly;
- include your CCTV system as part of your induction process for new staff, so they know who is responsible and what effect it may have on them;
- provide basic training in the system for all staff who may need to explain the CCTV system to customers. This also makes sure they know how it may affect them;
- ensure all staff have easy access to your CCTV policy; and

- ensure staff are aware that they need to protect people's privacy and what will happen if they do not (eg disciplinary procedures for unjustifiably accessing or using information).

# 3. Selecting and positioning cameras

When you come to choosing cameras, equipment and technology, constantly refer back to your purpose for having CCTV. This will help you to comply with **principles 1, 10** and **11** (these principles are explained under sections 1 and 6).

For example, if your main purpose for using CCTV is to get evidence to detect if an employee takes money from a till, the image will need to be clear enough to be able to be used as evidence against a person if necessary. Or, if your purpose is to monitor pedestrian traffic exiting and entering a large stadium so you can respond to overcrowding or delays, you will not need high resolution cameras that can identify people's faces – you simply need equipment that will let you check the movement of the crowds.

When positioning the cameras, make sure you do not collect personal information in a way that will intrude to an unreasonable extent on the privacy of the individual (**principle 4**). Using CCTV in bathrooms or change areas is highly likely to breach this principle.

## Guidelines

3.1 Choose equipment which will achieve the purpose of your system in the most privacy friendly way.

3.2 Where feasible, also use 'privacy enhancing technologies'.

3.3 Position cameras in a way that will not intrude to an unreasonable extent on the privacy of individuals.

### Guideline 3.1 – Choosing the right equipment

You need to take privacy into account when you choose your equipment. Some types of systems have relatively little effect on privacy, and others are highly intrusive. The more privacy intrusive your system is, the more careful you will have to be with managing it.

Some of the things you need to think about when choosing your cameras include:

- **Image quality**: Make sure you take into account image size, resolution and frames per second when choosing equipment and setting up your system. Bigger and clearer CCTV images are not always better. The more identifiable a person is, the more you have to think about privacy – and the more you capture, the more storage space the images will take. So only collect the amount and quality of footage you need. This will fit in with **principle 1** (see section 1).

  For example, if you are using CCTV to capture evidence of a crime you may need more frames per second to ensure you clearly capture the movement and action of an individual to use as evidence in criminal proceedings. However, if you are only using your CCTV to alert you to the fact that someone is entering a restricted space, so that you can then respond, a low number of frames per second will probably suffice.

- **Zoom and rotation**: Zoom and rotation functions can help people monitoring CCTV cameras identify people and objects that are far away or swivel cameras to follow a particular incident across space.

  However, be careful to make sure that zoom and rotation does not allow filming of private spaces that lie alongside the public or semi public spaces under surveillance by your system (such as a person's backyard). If possible, configure your cameras so that they are unable to turn towards private spaces. If you use zooming and rotating cameras, you should also have systems in place to oversee and audit the use of camera zoom and rotation by staff. You need to make sure staff are not misusing it. And if your system may cause concern for your neighbour, discuss it with them, and show them how it works so you can reassure them.

- **Fixed or portable cameras**: If you choose to install portable cameras that you move around at intervals, you will need to ensure that signage for the cameras is also moved. If the cameras move to a location far from the original location, you may need to do a new evaluation (see guideline 1.2). As much as possible, try to anticipate at the start where you might want to put the cameras.

- **Wired or wireless connections**: Generally, wired connections are more secure than wireless connections. So if you opt for wireless technology to connect your cameras and your monitor or control room, make sure you transmit images in an encrypted form.

- **Intelligent surveillance technology**: Intelligent surveillance technology allows CCTV images to be analysed for certain activities, objects or people. 'Automated face recognition' is an example of an intelligent surveillance technology. Intelligent surveillance technologies can be used in privacy friendly ways. For example, technologies that allow cameras to go unmonitored and only record particular types of events (such as movement in a restricted area or unattended objects) may allow your cameras to record less frequently and therefore have less impact on individuals' privacy.

**Guideline 3.2 – Using privacy enhancing technologies**

Privacy enhancing technologies – also known as 'PETs' – are technologies specifically designed to help to protect individuals' privacy and personal information. PETs can add to the efficiency of your system by making it easier to comply with privacy law and reducing people's worries over privacy.

An everyday example of a PET is encryption technology. Encryption protects personal information from being seen or used by others who are not the intended owners or recipients of the information. It can be used for such things as securing wireless connections, or protecting CCTV images stored in your system. Encryption is an easy method of protecting privacy, which is accessible for organisations of all sizes.

There are also new technologies available specifically for CCTV – though, because of their current cost, they may be particularly suitable for larger systems. For instance, technology developed at the University of Toronto blurs the images of people appearing in CCTV footage. This allows staff to monitor CCTV footage without being able to identify people. If it is necessary to identify a person in the footage, this can be done either in real-time or after the images are recorded, but only by an appropriate person with a decryption "key". These types of technologies will gradually become cheaper and so more accessible to ordinary CCTV users.

**Guideline 3.3 – Avoiding intrusive camera locations**

Take care where you place your CCTV cameras. You need to avoid unreasonably intruding on people's privacy. It is almost certainly going to be seen as unreasonably intrusive if you have cameras pointing at or into bathrooms, changing rooms, a person's private front or backyard or any other places where people are likely to expect privacy. Also be careful to avoid placing cameras in positions where they point through windows, regardless of whether the building is a private residence or a publicly accessible building.

You may also need to take care with where cameras point in public spaces. For example, cameras that point towards the entrance of a women's refuge or a sexual health clinic will raise considerable privacy issues.

# 4. Make people aware of the CCTV

Under **principle 3** of the Privacy Act, you need to make individuals aware that you are collecting their personal information and why. So you need to provide what is sometimes called a 'collection notice' or a 'privacy notice'.

A privacy notice will tell people:

- that the information is being collected;
- the purpose for which the information is being collected;
- if you intend to pass the information on to others, and if so to whom;
- your name and address;
- whether the collection of the information is authorised or required under a particular law; and
- the rights of the individual to access and correct the information.

Principle 3 is intended to make sure people know what is happening with their information so they are in a better position to protect and manage their privacy.

Of course, it will not always be practical or appropriate to include all this information in the signs that you display near your CCTV cameras. Your signs are likely to be brief. However, use additional methods to give people more detailed information (these are explained below).

Signage is not just something you have to do to comply with the law. It makes sense for your business. For instance, if your CCTV is aimed at deterring crime, letting people know it is operating is an essential part of fulfilling that purpose.

## Guidelines

4.1 Erect signs both near the CCTV cameras and at the perimeter of the CCTV system's range (before individuals enter the range of the cameras) to notify people that cameras are operating.

4.2 The signs should make clear who owns and operates the CCTV system and the contact details of that agency (if this information is not already obvious).

4.3 Make sure there is a full privacy notice on your website, or in hard copy at your reception desk, to let the public know more about the operation of the CCTV cameras. If you are installing a system with a major public impact (such as a local council scheme), put notices in the media.

4.4 Ensure your staff can answer questions from the public about the system.

**Guidelines 4.1 and 4.2 – CCTV signage**

Ideally, people should know about the CCTV cameras before they get close enough to be filmed by them. Make sure you take this into account when choosing sites for signs. You should also have a sign close to where the actual camera is.

For CCTV operated indoors, make sure there are signs at the entrances to the building.

The signs should be simple and clear.

- They should briefly describe why the CCTV system is being used. For instance, it is common for signs to say 'crime prevention cameras in operation', or 'traffic management cameras in operation'.
- It must be obvious whom people should contact for more information. For example, if the camera is operating in a single shop and the shop owner is the operator, it may not be necessary to give contact details. If the shop is part of a chain, however, the CCTV may well be managed by someone off-site so you need to provide contact details. These should include a phone number and, if applicable, a website address. This is also important for CCTV in public places where it is not obvious who is running and monitoring the cameras.

**Guideline 4.3 – Detailed CCTV notices**

The notices you place in the newspapers and on your website should contain all the additional information about the CCTV that you are required to give people under principle 3 (see above) but that cannot fit on your signs.

The New Zealand Police have an example of a CCTV public notice available at www.police.govt.nz/resources/2003/cctv/cctv-public-notice-example.html which could provide a useful model for your own notice.

Notices should be posted both at the time the system is about to start operating and at regular intervals during the life of the system to ensure the public continues to be aware of the existence of the cameras.

If you have a fairly specific clientele or customer base, you should consider raising awareness of the CCTV cameras through your mailing lists or newsletters.

**Guideline 4.4 – Make sure your staff can help if people ask for information**

You will already have trained your staff and made them aware of your CCTV policies (see guideline 2.5). Make things easy for them – for instance, give them some hard copies of the policies to hand out to customers if people ask them for information.

# 5. Collecting only necessary images

In the Privacy Act, **principles 1 to 4** are 'the collection principles'. In summary, they generally require that you:

- only collect the personal information necessary to achieve your purposes;
- only collect personal information for a lawful purpose and by lawful means;
- collect personal information directly from the individual (rather than from someone else);
- give individuals a 'privacy notice' which tells them who you are and why you are collecting their personal information; and
- collect personal information fairly and avoid methods that will intrude to an unreasonable extent on the individual.

Many of these collection principles have already been covered earlier in the guidelines. However, guideline 5.1 helps you comply with your obligation to collect only the information that is *necessary* for your purpose. Avoid the temptation to collect additional information just in case there may be use for it later.

## Guidelines

5.1 Limit the hours that the CCTV cameras operate to times where it is necessary (such as opening hours, or days and times during the week when crime peaks).

### Guideline 5.1 – Limit the hours when CCTV operates

Collecting only "necessary" information can be a challenge with CCTV cameras, because you usually do not know when a particular incident of interest might happen. However, your CCTV evaluation (under guideline 1.2) will help you to determine what is necessary.

For example:

- If you are using the CCTV to address crime, your evaluation will have analysed the type and number of crimes and when they usually occur. This will help you to determine when the cameras should be operating. So if you have cameras to address vehicle theft, and thefts are high on week nights but negligible during the day and at weekends, limit the times when you operate the cameras.
- If you are using the cameras to ensure the smooth flow of peak hour traffic, your cameras should only operate Monday to Friday during peak hours.
- If you operate a bar that is busy on Friday and Saturday nights but also has a live music night every Wednesday where patrons are known to become rowdy and sometimes violent, run your cameras on Wednesday, Friday and Saturday nights. You may not need to run them on your quieter nights when there are rarely any problems.

It pays to be careful about the amount of personal information you collect. Apart from the risk of breaching principle 1, it can be expensive. For example, if you collect information you do

not need, you can use up time and storage space collecting, storing and destroying information you do not use.

# 6. Using the CCTV images

In the Privacy Act, **principles 10 and 11** say that you may only use or disclose personal information for the purpose you collected it, or for a directly related purpose.

You risk breaching these principles if you collect personal information for one thing and then later use it for a different reason. An example of this is where an agency collects CCTV footage to deter vehicle theft in a car park and later provides footage from the cameras to a television station for an entertainment programme. Having a clear purpose for the CCTV will help you avoid this.

There are some exceptions to principles 10 and 11. For example, you may use or disclose personal information for another purpose if:

- the use or disclosure is necessary for court or tribunal proceedings;
- the use or disclosure is necessary to enable a public sector agency (often the Police) to uphold the law. This includes enabling them to prevent, detect, investigate, prosecute and punish offences. (See guideline 8.3 for further information on disclosing images to the Police);
- the use or disclosure is necessary to prevent or lessen a serious and imminent threat to public health and safety or the life and health of an individual; or
- the individual has consented to the use or disclosure.

**Principle 8** also says that you should take reasonable steps to check the accuracy of personal information before you use it. What are 'reasonable steps' will depend on the circumstances. For instance, if your use of the information is going to have an adverse impact on a person, it will be reasonable to go to more effort to check its accuracy.

## Guidelines

6.1 Take reasonable steps to check CCTV images are accurate, complete, relevant and not misleading before you use them.

6.2 Only use or disclose the images you collect with CCTV cameras for the original purpose you collected them.

6.3 Do not publicly disclose images collected using CCTV unless you have the consent of the individual(s) shown in the footage or you have consulted the Police.

6.4 Follow the policy you developed under guideline 2.4.

### Guideline 6.1 – Check the accuracy of CCTV footage

Although CCTV cameras capture a photographic record of an event or person, there is still the possibility that footage can be inaccurate, incomplete or misleading.

For example:

- If the date and time stamping on the footage is wrong, this can hinder investigations by leading to the wrong person being tracked down and questioned.
- Or the image might suggest that a person is a shoplifter where in fact that is not the case. Disclosing that image without checking its accuracy can cause the person serious embarrassment. You need to take great care before labelling someone as a criminal.
- Footage of an assault that does not show the moments before the person throws a punch may fail to show that that person was attacked first and was defending themselves.
- If images are too blurry or out of focus, they could be misleading and result in you targeting the wrong person. So take steps to ensure that images are of the appropriate quality for your purposes.

**Guideline 6.2 – Limits on use and disclosure of CCTV images**

Generally, under the Privacy Act, you should only use or disclose CCTV footage for the original purpose for which you collected it.

If you have followed these guidelines, you will have identified your purpose for using CCTV in your initial evaluation (guideline 1.2) and in your business plan (guideline 2.1). You will know to whom you might want to disclose the information. You will also have informed people of the purpose of the CCTV in your public notices about the cameras (guideline 4.3). So this obligation should not be at all difficult.

Once you have information, though, it can be tempting to use it for different purposes.

- For instance, if your purpose for using the CCTV is to catch shoplifters in your retail outlet, you may find out that it is also possible to use the footage for market research and analysis of customer shopping habits.

  However, this is a purpose that is unrelated to the one you told people about when you set up the system. So you cannot just use the CCTV for that purpose – it is too different from the original purpose.

  If you think that new purpose is now important to you, go back to the start of these guidelines and work through the evaluation, business plan and notification stages again. You are proposing to change your system substantially, so do it properly.

Some purposes are very closely connected to your original stated purpose. If this is the case, there is no problem with using or disclosing the information for those purposes.

- For example, suppose that your purpose for having CCTV is to “detect and prosecute shoplifting”. If your CCTV shows a person shoplifting in your retail outlet, you can use that footage to help security staff identify and apprehend the shoplifter while they are on the premises. And if the footage would help the Police in their investigations, you can give the footage to the Police. These uses and disclosures are clearly and closely linked with the purpose of detecting and prosecuting shoplifters.

The exceptions listed in the Privacy Act (see Appendix B for full details) also allow you to disclose CCTV images if:

- the use or disclosure is necessary for court or tribunal proceedings;

- the use or disclosure is necessary to enable a public sector agency to uphold the law (including preventing, detecting, investigating, prosecuting and punishing offences);
- the use or disclosure is necessary to prevent or lessen a serious and imminent threat to public health and safety or the life and health of an individual; or
- you have the consent of the people in them.

**Guideline 6.3 – Avoid public disclosure of CCTV images**

It is often difficult to justify public disclosure of CCTV images. By 'public disclosure' we mean releasing information to the public at large (not to a single agency such as the Police or to an individual).

Public disclosure includes:

- publishing still CCTV images in a newspaper or in the window of your premises;
- uploading footage to the internet;
- circulating it widely to an email group; or
- placing images on a workplace notice board where non-staff members may see it.

Releasing CCTV footage to the public can have a serious impact on the privacy of the individuals in the footage. For example, once something is uploaded to the internet, it can be difficult if not impossible to remove that information. Even if the individual in the footage is in the wrong, it is better to contact the Police and seek their advice. If you publicly release footage you may breach the Privacy Act or interfere with Police investigations.

The Police may publicly release CCTV images to investigate a crime, or to help identify or locate a person who is in danger or who is a danger to others. If you think that your CCTV images need to be released publicly for whatever reason, go to the Police. The Police will have the appropriate information to decide whether releasing the footage is necessary.

**Guideline 6.4 – Use CCTV in accordance with your policy**

It is surprising how many agencies have policies but do not follow them.

Under guideline 2.4, you will have developed a CCTV policy that should explain exactly how CCTV images will be used in your agency. As a reminder, make sure that:

- the policy is practical and easy for you and your staff to follow (if it is difficult, or people do not understand why it is there, they will ignore it);
- you continue to check that the policy is being followed; and
- all staff know about the policy and how to follow it.

# 7. Storage and retention of images

**Principle 5** of the Privacy Act relates to the security of information. It says that agencies must protect personal information from loss and from unauthorised access, use, modification and disclosure. This also makes sense at a business level. Security breach incidents can seriously damage and even destroy the reputation of your business or organisation.

So you need technological and procedural steps in place to protect footage collected using CCTV.

**Principle 9** says that you must not keep personal information for longer than you need for the purposes for which you collected it. In other words, if you collected personal information for a particular purpose and that purpose has passed or you have finished using the information, you must delete or destroy it.

## Guidelines

7.1 Ensure that CCTV images are protected from loss and unauthorised access, use, modification and disclosure.

7.2 Only keep CCTV images for a specified time. This time period must not be longer than is necessary to achieve your purpose.

### Guideline 7.1 – Protecting CCTV images

Security arrangements are essential to avoid or lessen the possibility that personal information is lost or inappropriately accessed or released. Treat footage as **confidential**.

Your safeguards can be both technical and procedural. Some **technical safeguards** include:

- having an audit trail (or electronic footprints) so you can monitor staff access to footage;
- using password protection to manage staff access to stored footage;
- transmitting and storing footage in encrypted form;
- encrypting any footage stored on removable storage devices (such as disks and USB sticks); and
- securely deleting or writing over footage you no longer need.

**Procedural safeguards** for CCTV footage include:

- limiting the number of staff who can access footage to those who 'need to know';
- ensuring confidentiality is part of your staff's contractual obligations and that there are penalties for breach;
- limiting access to your control room (if you have one – for more detail, see guideline 8.1);
- prohibiting the removal of footage from your premises on removable storage devices except in very limited circumstances (for example, in order to provide footage to Police);
- using physical barriers to secure footage and monitors. For instance, keep the tapes or storage media in locked rooms or cabinets; and
- doing regular audits of system security.

### Guideline 7.2 – Retention of footage

Under the Privacy Act you are not permitted to hold onto information indefinitely 'just in case' you might want to use it in the future.

Unless you need to keep CCTV footage so you can fulfil the purpose for which you use the CCTV cameras (such as keeping evidence of a crime), you should permanently delete the footage after a specified time. You will need to determine what the appropriate length of time should be for your system to achieve its purpose. Keep storage time to a minimum.

For example:

- If your purpose for using CCTV is to detect and prevent vehicle theft in a car park then you would need to keep the footage long enough for any thefts to be reported (say, a few days if it is a short-term park). You should then delete the images if you do not receive any reports.
- Any footage that shows a crime can be kept as long as it is needed to undertake criminal proceedings. It can then be deleted (check with the Police to ensure you do not delete information that they need for their case).
- If your purpose for using CCTV is to detect and prevent fraud being carried out at ATMs, you may need to retain footage for long enough for people to receive their bank statements and alert their bank to a suspicious transaction.

As explained in guideline 6.2 on the use and disclosure of images, there are exceptions listed in the Privacy Act that allow you to use images for something other than your original purpose. This might include giving them to the Police for law enforcement purposes. Because it is lawful to hold the information for these purposes, you can retain the images for long enough to achieve those purposes.

For example, if a crime has been reported to the Police that relates to something you recorded with your CCTV cameras, you will need to keep your footage for long enough for the Police to collect it from you.

# 8. Controlling who can see the images

One of your obligations under **principle 5** is to protect personal information from unauthorised access. This means protecting both stored CCTV footage and the area where monitoring of CCTV takes place.

Individuals have the right to access the personal information you hold about them **(principle 6)**. So, if an individual asks for access to CCTV footage and that footage is 'readily retrievable' you usually have to provide it.

If there are other identifiable people in the footage, you will need to look at options to protect those people's privacy.

Under **principle 7**, a person may also ask that their information be corrected if it is wrong.

If you are showing or giving CCTV footage to others who are not the subject of the footage, **principle 11** (disclosure of personal information) is relevant.

As discussed under earlier guidelines, you should generally treat CCTV footage as confidential to your organisation, and not disclose unless this is one of your purposes. However, if you want to give footage to the Police this will usually be fine because the disclosure will either be:

- directly related to the purpose you set up the CCTV for (eg investigation of crime); or

- a disclosure to a public sector agency so it can uphold the law (eg by prosecuting offences).

## Guidelines

8.1 Ensure that the control or monitoring room is only accessible by authorised staff members.

8.2 Establish procedures for individuals to access images of themselves captured by your CCTV cameras.

8.3 Establish procedures for when and how you disclose your CCTV images to the Police.

8.4 Keep a log of all instances where an external party has accessed CCTV images.

### Guideline 8.1 – Entry to the control room or monitoring area

If you have a CCTV monitoring room, it should only be entered by monitoring staff and other appropriate authorised people.

Sometimes small premises, such as small shops, have CCTV screens visible to customers. This is fine if the screens only show what the customers can already see by looking around them. However, if the premises are larger you will need to take more care. For instance, if a hotel has CCTV monitors in the reception area that show hotel guests in other parts of the building, those monitors should not be viewable by the guests in the reception area. The hotel should either move the monitors to somewhere more private, or turn the screens so that they are only viewable by the people behind the desk.

### Guideline 8.2 – Individuals can access images of themselves

It is common for people to ask to see – or even ask to have copies of – information from CCTV about themselves. So you need to have procedures in place to deal with these requests.

Generally, people have a right to access images of themselves. However, there are good reasons to refuse a request in some cases.

For instance, you do not need to provide access if the information is not 'readily retrievable'. So, if an individual asks for footage of him or herself, but cannot provide a specific time or location, then this information might well not be readily retrievable.

When giving access, you must also be careful not to intrude on the privacy of others captured in the footage. Think about how you are providing access. Your starting point is to give access in the way the individual concerned wants. However, this is not always possible or desirable:

- Giving someone a copy of the footage has different privacy impacts from just allowing someone to come in and view the footage. For instance, it may not be a problem to let someone view a tape. However, there may be a good reason not to provide a copy if the information could be damaging or embarrassing for others who are pictured if it is put on the internet.
- If you have the technology to blur or pixellate the faces of the other people on a copy of the footage, this is a good way to protect others' privacy.

- If you cannot provide access to the footage without unreasonably breaching others' privacy, you could provide the individual with a written description of what they are doing in the footage.

You should develop procedures to deal with these issues and include these in the policy you develop under guideline 2.4. Use this to develop a checklist for staff on how to handle a request for access, setting out for example:

- how much time the staff member has to respond to the request (you must respond as soon as possible, but within a maximum of 20 working days);
- how the staff member will confirm that the person requesting access to the footage is actually the person featured in the footage;
- whether the staff member should provide a copy of the footage, a description of the footage, or require the person to come in to view the footage; and
- that, if the images are connected to a criminal investigation, the staff member should check with the Police before granting access to the footage.

**Guideline 8.3 – Disclosing your CCTV footage to the Police**

As explained above, you can usually disclose CCTV footage to the Police. You do not *have* to do so, unless the Police have a warrant for the information or there is a law requiring you to disclose. However you will often be willing to co-operate with the Police.

It is still a good idea to have a paper-trail, showing how you have dealt with requests by the Police. This will help you manage the requests properly, and will also demonstrate to anyone who later asks (for instance the Privacy Commissioner) why you disclosed the information.

Access to footage should not be ad hoc or unplanned, otherwise you might inadvertently find yourself in breach of the Privacy Act. So take the time to develop a procedure for giving Police access and make sure it is included in your CCTV policy developed under guideline 2.4.

The easiest way to do this is to have a simple form that the Police fill out if they want to access your CCTV footage. The form should ask specific questions about:

- the event the Police are interested in;
- the location where they think the event took place;
- the approximate time the event took place;
- the specific offence being investigated;
- the name and contact details of the Police Officer making the request; and
- the date of the request.

Once you have made a decision about the Police's request, you can then also note that on the form.

If you work with the Police regularly, it may be appropriate to have an agreement in place with them, such as a Memorandum of Understanding. For example, local councils may either own cameras that the Police monitor, or have staff who work with Police officers to monitor the cameras. The agreement can clearly set out the roles of the different parties and how access to footage will be managed.

**Guideline 8.4 – Keep a log of access to CCTV**

It is worth keeping a log of the people whom you allow to access your CCTV (including the Police and individuals), as well as the details of the request and the reason you agreed to provide access. You should also log the details of requests for access where you decided not to provide access.

Having a log helps you stay in control of disclosures of CCTV footage. Importantly, it also provides a record of your decisions if you are later asked to justify your decision whether to release CCTV footage. It is much simpler (and cheaper) to keep a log at the time than to try to remember later why you made a decision or who a particular requester was.

# 9. Audit and evaluation

Your initial evaluation of the need for CCTV (under guideline 1.2) helped you determine whether CCTV was necessary. You should continue to evaluate the need for CCTV and how you are running it to ensure you continue to comply with the privacy principles.

Audits and evaluations are also a good business practice to ensure you are getting value from your investment. Audits help ensure good information handling and the fast identification of problems.

## Guidelines

9.1 Collect statistics about your CCTV system to allow you to assess its strengths and weaknesses.

9.2 After a year of operation and at regular intervals afterwards, evaluate the operation of the system to determine its effectiveness and continuing viability.

9.3 Do regular audits of your equipment and procedures to ensure the system is operating smoothly.

9.4 Check that your staff or CCTV operators are complying with your policies, and retrain as required.

**Guideline 9.1 – Collect statistics**

It is important to collect statistics about your CCTV system to help you assess its strengths and weaknesses and its general performance from month to month and year to year. Depending on the purpose of the cameras, you may wish to collect statistics or other information on:

- the number of incidents captured by the cameras;
- the types of incidents recorded by the cameras;
- the time/days of the week when incidents occurred;
- which cameras captured the most and the fewest incidents;
- the numbers and types of camera problems or repairs;
- the amount of money you spend on your CCTV system; and

- how many requests for access to CCTV you received and, of these, how many times you provided access to CCTV.

**Guideline 9.2 – Regularly evaluate the system's effectiveness**

Do a complete evaluation of your system's effectiveness at regular intervals. Although your system might be effective in the first year, in later years its success might taper off or be affected by other factors.

Repeating an evaluation is usually not onerous. Often, the same issues that were relevant for your initial evaluation will help you in your ongoing evaluations.

You may also need to assess whether you need to upgrade the system. For example, do you need to upgrade the technology you are using or move some of your cameras to get better results?

**Guideline 9.3 – Check equipment and procedures**

You should also do regular audits of the system as a whole to make sure it is running as it should. Checking equipment will allow you to respond quickly to mechanical failures and cameras in disrepair. Audits of equipment can include checking:

- camera zoom function;
- camera rotation function and whether it moves back to a 'home position';
- camera recording function and whether it is occurring at the right time;
- the image quality of recordings and whether it is at the appropriate standard;
- security of the transmission, storage and deletion of CCTV footage; and
- the performance of any 'intelligent surveillance technologies'.

**Guideline 9.4 – Regularly check that your policies are being followed**

You should also make sure your staff or CCTV operators are following the CCTV policy you developed under guideline 2.4. You may need to do this fairly frequently, depending on the size of your CCTV system and the number of people involved.

Take the opportunity to remind your staff of the policies and do any retraining that is required.

In doing this, make sure you check the audit trails that record which staff have accessed footage and the way cameras are used by staff.

Review the policies regularly too. Are they still easy for your staff to follow? Do they explain clearly enough for your customers or others what you are doing?

# Appendix A: CCTV checklist for small businesses

This checklist is for small businesses that operate or intend to operate small CCTV systems of a low number of cameras. **You should review the checklist regularly**.

Before you start, you need to have identified a clear reason for having a CCTV system. This is your purpose – see Section 1 and Guideline 1.1 for more details.

| **Purpose** | | | | |
|---|---|---|---|---|
| ***Relevant guidelines*** | ***Actions and practices*** | ***Date checked*** | ***By*** | ***Date of next review*** |
| **Section 2** Guideline 2.3 | **Responsibility:** There is a named individual who is responsible for the operation of the system. | | | |
| **Section 3** Guideline 3.1 | **Equipment:** You have chosen CCTV cameras and other equipment that are suitable for your purpose (outlined above) and they are operating properly. | | | |
| **Section 3** Guideline 3.3 | **Unintrusive camera locations:** The CCTV cameras are not located in places that intrude on the privacy of individuals (such as bathrooms, backyards, through windows etc). | | | |
| **Section 4** Guideline 4.2 and 4.3 | **Signage:** There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system, your name and contact details are displayed on the signs. | | | |
| **Section 5** Guideline 5.1 | **Limits to time when cameras operate:** CCTV cameras only operate when necessary, such as during opening hours or days and times of the week when crime peaks. | | | |
| **Section 6** Guideline 6.2 | **Use and disclosure of CCTV images:** You only use or disclose CCTV footage for the purpose outlined above and not for any other reason. | | | |
| **Section 7** Guideline 7.1 | **Security of CCTV images:** Images are transmitted and stored securely. | | | |
| **Section 7** Guideline 7.2 | **Limited retention periods:** Recorded CCTV images are kept for a specified time. This time period must not be longer than is necessary to achieve your purpose outlined above. | | | |
| **Section 8** Guideline 8.2 | **Access to CCTV images by individuals:** Individuals can access CCTV images of themselves, but you also protect the privacy of others in the footage. | | | |
| **Section 8** Guideline 8.4 | **Log of access:** You keep a log of who has accessed your CCTV footage, including access by individuals and the Police. | | | |
| **Section 9** Guideline 9.3 | **Regular review:** You do regular checks to ensure the system is working properly. | | | |

# Appendix B: Privacy Act principles

*Information Privacy Principles*

Principle 1 Purpose of collection of personal information

Personal information shall not be collected by any agency unless—

(a) The information is collected for a lawful purpose connected with a function or activity of the agency; and

(b) The collection of the information is necessary for that purpose.

Principle 2 Source of personal information

(1) Where an agency collects personal information, the agency shall collect the information directly from the individual concerned.

(2) It is not necessary for an agency to comply with subclause (1) of this principle if the agency believes, on reasonable grounds,—

- (a) That the information is publicly available information; or
- (b) That the individual concerned authorises collection of the information from someone else; or
- (c) That non-compliance would not prejudice the interests of the individual concerned; or
- (d) That non-compliance is necessary—
  - (i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or
  - (ii) For the enforcement of a law imposing a pecuniary penalty; or
  - (iii) For the protection of the public revenue; or
  - (iv) For the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
- (e) That compliance would prejudice the purposes of the collection; or
- (f) That compliance is not reasonably practicable in the circumstances of the particular case; or
- (g) That the information—
  - (i) Will not be used in a form in which the individual concerned is identified; or
  - (ii) Will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
- (h) That the collection of the information is in accordance with an authority granted under section 54 of this Act.

Principle 3 Collection of information from subject

(1) Where an agency collects personal information directly from the individual concerned, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of—

- (a) The fact that the information is being collected; and
- (b) The purpose for which the information is being collected; and
- (c) The intended recipients of the information; and
- (d) The name and address of—
  - (i) The agency that is collecting the information; and
  - (ii) The agency that will hold the information; and

(e) If the collection of the information is authorised or required by or under law,—
  (i) The particular law by or under which the collection of the information is so authorised or required; and
  (ii) Whether or not the supply of the information by that individual is voluntary or mandatory; and
(f) The consequences (if any) for that individual if all or any part of the requested information is not provided; and
(g) The rights of access to, and correction of, personal information provided by these principles.

(2) The steps referred to in subclause (1) of this principle shall be taken before the information is collected or, if that is not practicable, as soon as practicable after the information is collected.

(3) An agency is not required to take the steps referred to in subclause (1) of this principle in relation to the collection of information from an individual if that agency has taken those steps in relation to the collection, from that individual, of the same information or information of the same kind, on a recent previous occasion.

(4) It is not necessary for an agency to comply with subclause (1) of this principle if the agency believes, on reasonable grounds,—
(a) That non-compliance is authorised by the individual concerned; or
(b) That non-compliance would not prejudice the interests of the individual concerned;
(c) That non-compliance is necessary—
  (i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or
  (ii) For the enforcement of a law imposing a pecuniary penalty; or
  (iii) For the protection of the public revenue; or
  (iv) For the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
(d) That compliance would prejudice the purposes of the collection; or
(e) That compliance is not reasonably practicable in the circumstances of the particular case; or
(f) That the information—
  (i) Will not be used in a form in which the individual concerned is identified; or
  (ii) Will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

<u>Principle 4 Manner of collection of personal information</u>

Personal information shall not be collected by an agency—

(a) By unlawful means; or
(b) By means that, in the circumstances of the case,—
  (i) Are unfair; or
  (ii) Intrude to an unreasonable extent upon the personal affairs of the individual concerned.

<u>Principle 5 Storage and security of personal information</u>

An agency that holds personal information shall ensure—

(a) That the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against—
  (i) Loss; and

(ii) Access, use, modification, or disclosure, except with the authority of the agency that holds the information; and
(iii) Other misuse; and

(b) That if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

Principle 6 Access to personal information

(1) Where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled—
(a) To obtain from the agency confirmation of whether or not the agency holds such personal information; and
(b) To have access to that information.

(2) Where, in accordance with subclause (1)(b) of this principle, an individual is given access to personal information, the individual shall be advised that, under principle 7, the individual may request the correction of that information.

(3) The application of this principle is subject to the provisions of Parts 4 and 5 of this Act.

Principle 7 Correction of personal information

(1) Where an agency holds personal information, the individual concerned shall be entitled—
(a) To request correction of the information; and
(b) To request that there be attached to the information a statement of the correction sought but not made.

(2) An agency that holds personal information shall, if so requested by the individual concerned or on its own initiative, take such steps (if any) to correct that information as are, in the circumstances, reasonable to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete, and not misleading.

(3) Where an agency that holds personal information is not willing to correct that information in accordance with a request by the individual concerned, the agency shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the information, in such a manner that it will always be read with the information, any statement provided by that individual of the correction sought.

(4) Where the agency has taken steps under subclause (2) or subclause (3) of this principle, the agency shall, if reasonably practicable, inform each person or body or agency to whom the personal information has been disclosed of those steps.

(5) Where an agency receives a request made pursuant to subclause (1) of this principle, the agency shall inform the individual concerned of the action taken as a result of the request.

Principle 8 Accuracy, etc, of personal information to be checked before use

An agency that holds personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.

Principle 9 Agency not to keep personal information for longer than necessary

An agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.

Principle 10 Limits on use of personal information

An agency that holds personal information that was obtained in connection with one purpose shall not use the information for any other purpose unless the agency believes, on reasonable grounds,—

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

Principle 11 Limits on disclosure of personal information

An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds,—

(a) That the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or
(b) That the source of the information is a publicly available publication; or
(c) That the disclosure is to the individual concerned; or
(d) That the disclosure is authorised by the individual concerned; or
(e) That non-compliance is necessary—
    (i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or
    (ii) For the enforcement of a law imposing a pecuniary penalty; or
    (iii) For the protection of the public revenue; or
    (iv) For the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
(f) That the disclosure of the information is necessary to prevent or lessen a serious and imminent threat to—
    (i) Public health or public safety; or
    (ii) The life or health of the individual concerned or another individual; or

(g) That the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern; or

(h) That the information—

(i) Is to be used in a form in which the individual concerned is not identified; or

(ii) Is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(i) That the disclosure of the information is in accordance with an authority granted under section 54 of this Act.

Principle 12 Unique identifiers

(1) An agency shall not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the agency to carry out any one or more of its functions efficiently.

(2) An agency shall not assign to an individual a unique identifier that, to that agency's knowledge, has been assigned to that individual by another agency, unless those 2 agencies are associated persons within the meaning of subpart YB of the Income Tax Act 2007 (to the extent to which those rules apply for the whole of that Act excluding the 1973, 1988, and 1990 version provisions).

(3) An agency that assigns unique identifiers to individuals shall take all reasonable steps to ensure that unique identifiers are assigned only to individuals whose identity is clearly established.

(4) An agency shall not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned or for a purpose that is directly related to one of those purposes.