# 1. Foreword

CCTV surveillance has become a common feature of our daily lives. We are caught on numerous CCTV cameras as we move around our towns and cities, visit shops and offices, and travel on the road and other parts of the public transport network. Whilst the use of CCTV continues to enjoy general public support, it necessarily involves intrusion into the lives of ordinary individuals as they go about their day to day business. Our research has shown that the public expect it to be used responsibly with effective safeguards in place. Maintaining public trust and confidence in its use is essential if its benefits are to be realised and its use is not to become increasingly viewed with suspicion as part of a surveillance society.

This code of practice replaces one first issued in 2000. Since then there have been advances in the way CCTV is used, the technology employed and the wider legal environment in which it operates. There have also been developments which may help achieve more privacy friendly ways of using CCTV. This revised code builds upon the previous guidance reflecting these changes and the lessons learnt of how it is used in practice. During the production of the code discussions have taken place with organisations that use CCTV and a public consultation exercise undertaken which generated many valuable comments.

However, the objective of this code remains the same: helping ensure that good practice standards are adopted by those who operate CCTV. If they follow its provisions this not only helps them remain within the law but fosters public confidence by demonstrating that they take their responsibilities seriously.

# 2.About this code

This code provides good practice advice for those involved in operating CCTV and other devices which view or record images of individuals. It also covers other information derived from those images that relates to individuals (for example vehicle registration marks). This code uses the terms 'CCTV' and 'images' throughout for ease of reference. Information held by organisations that is about individuals is covered by the Data Protection Act 1998 (DPA) and the guidance in this code will help operators comply with their legal obligations under the DPA.

The DPA not only creates obligations for organisations, it also gives individuals rights, such as the right to gain access to their details and to claim compensation when they suffer damage.

The basic legal requirement is to comply with the DPA itself. This code sets out the Information Commissioner's recommendations on how the legal requirements of the DPA can be met. Organisations may use alternative methods to meet these requirements, but if they do nothing then they risk breaking the law.

The recommendations in this code are all based on the legally enforceable data protection principles (Appendix 1) that lie at the heart of the DPA and they have been set out to follow the lifecycle and practical operation of CCTV. Each section of the code poses questions that must be positively addressed to help ensure that the good practice recommendations are being achieved.

Following the recommendations in this code will:

- help ensure that those capturing images of individuals comply with the DPA;
- mean that the images that are captured are usable; and
- reassure those whose images are being captured.

This code replaces the earlier code of practice issued by the Information Commissioner's Office (ICO) in 2000 (reprinted in 2001) and the supplementary guidance for small users. It takes account of the technical, operational and legal changes that have taken place since the original code was drawn up.

CCTV operators and practitioners have been involved in its production and we have taken into account their experiences of using the previous code of practice. It also builds upon research the ICO has commissioned into public attitudes to surveillance technologies and research on 'surveillance society' issues more generally.

# 3. What this code covers

This code covers the use of CCTV and other systems which capture images of identifiable individuals or information relating to individuals for any of the following purposes:

- Seeing what an individual is doing, for example monitoring them in a shop or walking down the street.
- Potentially taking some action in relation to an individual, for example handing the images over to the police to investigate a crime.
- Using the images of an individual in some way that will affect their privacy, for example passing images on to a TV company.

Most CCTV is directed at viewing and/or recording the activities of individuals. This means that most uses of CCTV by organisations or businesses will be covered by the Data Protection Act (DPA) and the provisions of this code, regardless of the size of the system. This replaces our previous guidance on when a CCTV system has to comply with the DPA.

The use of cameras for limited household purposes is exempt from the DPA. This applies where an individual uses CCTV to protect their home from burglary, even if the camera overlooks the street or other areas near their home. Images captured for recreational purposes, such as with a mobile phone, digital camera or camcorder, are also exempt.

**Example:** If you make a video of your child in a nativity play for your own family use, this is not covered by data protection law.

This code is primarily aimed at businesses and organisations who routinely capture images of individuals on their CCTV equipment. Some specific uses of image recording equipment are not intended to be covered in this code, although they may still be covered by the requirements of the DPA.

- The covert surveillance activities of the law enforcement community are not covered here because they are governed by the Regulation of Investigatory Powers Act (RIPA) 2000 and Regulation of Investigatory Powers (Scotland) Act (RIPSA) 2000.
- The use of conventional cameras (not CCTV) by the news media or for artistic purposes such as for film making are not covered by this code as they are subject to special treatment in the DPA. This code does apply to the passing on of CCTV images to the media.

Not all sections of the code will be fully relevant to all CCTV systems; this will depend upon the extent and use of the images. Although small-scale users (such as small retailers) are covered by the DPA, they are unlikely to have sophisticated systems, so many of this code's provisions are inappropriate. Appendix 2 provides special guidance, as an alternative to the full code, for very limited use of CCTV where privacy risks are small and resources are limited. If you are a small user, but you wish to use your CCTV system for any purpose which is not covered in the checklist, you should read the full code. Appendix 3 is for employers who may use CCTV to monitor their workers.

**Note:** The DPA applies to images captured by CCTV. This code does not cover the use of dummy or non-operational cameras.

# 4. Deciding whether to use CCTV or continue using CCTV

Using CCTV can be privacy intrusive, as it is capable of putting a lot of law-abiding people under surveillance and recording their movements as they go about their day to day activities. You should carefully consider whether to use it; the fact that it is possible, affordable or has public support should not be the primary motivating factor. You should take into account what benefits can be gained, whether better solutions exist, and what effect it may have on individuals.

**Example:** Cars in a car park are frequently damaged and broken in to at night. Consider whether improved lighting would reduce the problem more effectively than CCTV.

You should consider these matters objectively as part of an assessment of the scheme's impact on people's privacy. This does not have to be an extensive or time-consuming process in all cases. The extent of assessment necessary will depend on the size of the proposed scheme and the level of impact it is likely to have on people's privacy[1].

You should use the results of the impact assessment to determine whether CCTV is justified in all the circumstances and if so how it should be operated in practice.

The things to cover in any impact assessment include:

- What organisation will be using the CCTV images? Who will take legal responsibility under the Data Protection Act (DPA)?[2]
- What is the organisation's purpose for using CCTV? What are the problems it is meant to address?
- What are the benefits to be gained from its use?
- Can CCTV technology realistically deliver these benefits? Can less privacy-intrusive solutions, such as improved lighting, achieve the same objectives?
- Do you need images of identifiable individuals, or could the scheme use other images not capable of identifying the individual?
- Will the particular equipment/system of work being considered deliver the desired benefits now and remain suitable in the future?
- What future demands may arise for wider use of images and how will you address these?
- What are the views of those who will be under surveillance?
- What could you do to minimise intrusion for those that may be monitored, particularly if specific concerns have been expressed?

Where the system will be operated by or on behalf of a public authority, the authority will also need to consider wider human rights issues and in particular the implications of the European Convention on Human Rights, Article 8 (the right to respect for private and family life). This will include:

- Is the proposed system established on a proper legal basis and operated in accordance with the law?
- Is it necessary to address a pressing need, such as public safety, crime prevention or national security?
- Is it justified in the circumstances?
- Is it proportionate to the problem that it is designed to deal with?

If this is not the case then it would not be appropriate to use CCTV.

1 If you are establishing a large system, or considering a use of CCTV which could give rise to significant privacy concerns, you may wish to consider using the ICO's Privacy impact assessment handbook.

2 If CCTV is used by a business or organisation, then it is the body that is legally responsible under the DPA (the "data controller"), not an individual member of staff.

# 5. Ensuring effective administration

Establishing a clear basis for the handling of any personal information is essential and the handling of images relating to individuals is no different. It is important to establish who has responsibility for the control of the images, for example, deciding what is to be recorded, how the images should be used and to whom they may be disclosed. The body which makes these decisions is called the data controller and is legally responsible for compliance with the Data Protection Act (DPA).

Where more than one organisation is involved, each should know its responsibilities and obligations. If both make decisions about the purposes and operation of the scheme, then both are responsible under the DPA. This may be the case, for example, where the police have a 'live feed' from a local authority-owned camera.

- Who has responsibility for control of the images and making decisions on how these can be used? If more than one body is involved have responsibilities been agreed and does each know its responsibilities?
- Has the body (or have the bodies) responsible notified the Information Commissioner's Office (ICO) that they are the data controller? Does the notification cover the purposes for which the images are used, the disclosures that are made and other relevant details?[3]
- If someone outside your organisation provides you with any processing services, for example editing the images, is a written contract in place with clearly defined responsibilities? This should ensure that the images are only processed in accordance with your instructions. The contract should also include guarantees about security, such as storage and the use of properly trained staff.

You will also need clear procedures to determine how you use the system in practice.

- Have you identified clearly defined and specific purposes for the use of images, and have these been communicated to those who operate the system?
- Are there clearly documented procedures, based on this code, for how the images should be handled in practice? This could include guidance on disclosures and how to keep a record of these. Have these been given to appropriate people?
- Has responsibility for ensuring that procedures are followed been allocated to an appropriate named individual? They should ensure that standards are set, procedures are put in place to meet these standards and they should make sure the system complies with this code and with legal obligations such as an individual's right of access.
- Are proactive checks or audits carried out on a regular basis to ensure that procedures are being complied with? This can be done either by you as the system operator or a third party.

You should review regularly whether the use of CCTV continues to be justified. You will have to renew your notification yearly, so this would be an appropriate time to consider the ongoing use of CCTV.

---

3 Please be aware that notification to the Commissioner does not in itself ensure that the system is compliant. You will still need to comply with the data protection principles (see appendix 1). Not all organisations need to notify. Current notification requirements can be found at www.ico.gov.uk/what_we_cover/data_protection/notification.aspx

# 6. Selecting and siting the cameras

Any CCTV images must be adequate for the purpose for which you are collecting them. It is essential that you choose camera equipment and locations which achieve the purposes for which you are using CCTV. Both permanent and movable cameras should be sited and image capture restricted to ensure that they do not view areas that are not of interest and are not intended to be the subject of surveillance, such as individuals' private property. The cameras must be sited and the system must have the necessary technical specification to ensure that images are of the appropriate quality.

**Example:** Check that a fixed camera positioned in winter will not be obscured by the growth of spring and summer foliage.

- Have you carefully chosen the camera location to minimise viewing spaces that are not of relevance to the purposes for which you are using CCTV?
- Where CCTV has been installed to deal with a specific problem, have you considered setting the system up so it only records at the time when the problem usually occurs? Alternatively, have you considered other privacy-friendly ways of processing images? For example, some systems only record events that are likely to cause concern, such as movement into a defined area. This can also save on storage capacity.
- Will the cameras be sited to ensure that they can produce images of the right quality, taking into account their technical capabilities and the environment in which they are placed?
- Is the camera suitable for the location, bearing in mind the light levels and the size of the area to be viewed by each camera?
- Are the cameras sited so that they are secure and protected from vandalism?
- Will the system produce images of sufficient size, resolution and frames per second?

In areas where people have a heightened expectation of privacy, such as changing rooms or toilet areas, cameras should only be used in the most exceptional circumstances where it is necessary to deal with very serious concerns. In these cases, you should make extra effort to ensure that those under surveillance are aware[4].

To judge the quality of images that will be necessary, you will need to take into account the purpose for which CCTV is used and the level of quality that will be necessary to achieve the purpose. The Home Office Scientific Development Branch[5] recommends identifying the needs of a CCTV system by using four categories:

- **Monitoring:** to watch the flow of traffic or the movement of people where you do not need to pick out individual figures.
- **Detecting:** to detect the presence of a person in the image, without needing to see their face.
- **Recognising:** to recognise somebody you know, or determine that somebody is not known to you.
- **Identifying:** to record high quality facial images which can be used in court to prove someone's identity beyond reasonable doubt.

Their guidance gives more detail on the quality of images needed for each of these purposes, and should be consulted when choosing equipment.

---

4 The use of signs is included in the section on Responsibilities

5 CCTV Operational Requirements Manual (v4.0 55/06), available from http://scienceandresearch.homeoffice.gov.uk/hosdb

# 7. Using the equipment

It is important that a CCTV system produces images that are of a suitable quality for the purpose for which the system was installed. If identification is necessary, then poor quality images which do not help to identify individuals may undermine the purpose for installing the system.

- Do the recorded pictures and prints as well as the live screens produce good clear pictures? This is important to ensure that there has not been an unacceptable loss of detail during the recording process.
- Have you considered the compression settings for recording material? In a digital system, a high level of compression will result in poorer picture quality on playback.
- Have you set up the recording medium in such a way that images cannot be inadvertently corrupted?
- Is there a regular check that the date and time stamp recorded on the images is accurate?
- If automatic facial recognition technology is being used, are the cameras placed so that facial images are clearly captured? Are the results of any match checked by people before any action is taken?
- Has a regular maintenance regime been set up to ensure that the system continues to produce high quality images?
- If a wireless transmission system is used, are sufficient safeguards in place to protect it from being intercepted?

CCTV must not be used to record conversations between members of the public as this is highly intrusive and unlikely to be justified. You should choose a system without this facility if possible. If your system comes equipped with a sound recording facility then you should turn this off or disable it in some other way.

There are limited circumstances in which audio recording may be justified, subject to sufficient safeguards. These could include:

- Audio based alert systems (such as those triggered by changes in noise patterns such as sudden shouting). Conversations must not be recorded, and operators should not listen in.
- Two-way audio feeds from 'help points' covered by CCTV cameras, where these are activated by the person requiring assistance.
- Conversations between staff and particular individuals where a reliable record is needed of what was said, such as in the charging area of a police custody suite[6].

- Where recording is triggered due to a specific threat, e.g. a ‘panic button’ in a taxi cab.

In the limited circumstances where audio recording is justified, signs must make it very clear that audio recording is being or may be carried out.

The use of audio to broadcast messages to those under surveillance should be restricted to messages directly related to the purpose for which the system was established.

- If there is an audio monitoring or recording capability has this been disabled?
- If an audio based alert system is being used are measures in place to prevent conversations being monitored or recorded?
- If there are audio communications with help points, are these initiated by those requiring assistance?
- If a message broadcast facility is used, are the messages limited to those consistent with the original purpose for establishing the system?

6 Police use of body-worn video devices (headcams) is covered by the Home Office guidelines, "Guidance for the police use of body-worn video devices”, produced in consultation with the ICO. See the Home Office police publications page, http://police.homeoffice.gov.uk/news-and-publications/

# 8. Looking after the recorded material and using the images

## 8.1 Storing and viewing the images

Recorded material should be stored in a way that maintains the integrity of the image. This is to ensure that the rights of individuals recorded by the CCTV system are protected and that the material can be used as evidence in court. To do this you need to carefully choose the medium on which the images are stored, and then ensure that access is restricted. You may wish to keep a record of how the images are handled if they are likely to be used as evidence in court. Finally, once there is no reason to retain the recorded images, they should be deleted. Exactly when you decide to do this will depend on the purpose for using CCTV.

Many modern CCTV systems rely on digital recording technology and these new methods present their own problems. With video tapes it was very easy to remove a tape and give it to the law enforcement agencies such as the police for use as part of an investigation. It is important that your images can be used by appropriate law enforcement agencies if this is envisaged. If they cannot, this may undermine the purpose for undertaking CCTV surveillance.

- How easy is it to take copies of a recording off your system when asked for by a law enforcement agency? Can this be done without interrupting the operation of the system?
- Will they find your recorded images straightforward to use?

- What will you do when recorded material needs to be taken away for further examination?

Viewing of live images on monitors should usually be restricted to the operator unless the monitor displays a scene which is also in plain sight from the monitor location.

**Example:** Customers in a bank can see themselves on a monitor screen. This is acceptable as they cannot see anything on the screen which they could not see by looking around them. The only customers who can see the monitor are those who are also shown on it.

**Example:** Monitors in a hotel reception area show guests in the corridors and lifts, i.e. out of sight of the reception area. They should be turned so that they are only visible to staff, and members of the public should not be allowed access to the area where staff can view them.

Recorded images should also be viewed in a restricted area, such as a designated secure office. The monitoring or viewing of images from areas where an individual would have an expectation of privacy should be restricted to authorised persons.

- Are your monitors correctly sited taking into account the images that are displayed?
- Is your monitor viewing area appropriate and secure?
- Where necessary is access limited to authorised people?

## 8.2 Disclosure

Disclosure of images from the CCTV system must also be controlled and consistent with the purpose for which the system was established. For example, if the system is established to help prevent and detect crime it will be appropriate to disclose images to law enforcement agencies where a crime needs to be investigated, but it would not be appropriate to disclose images of identifiable individuals to the media for entertainment purposes or place them on the internet. Images can be released to the media for identification purposes; this should not generally be done by anyone other than a law enforcement agency.

**NOTE:** Even if a system was not established to prevent and detect crime, it would still be acceptable to disclose images to law enforcement agencies if failure to do so would be likely to prejudice the prevention and detection of crime.

Any other requests for images should be approached with care, as a wide disclosure of these may be unfair to the individuals concerned. In some limited circumstances it may be appropriate to release images to a third party, where their needs outweigh those of the individuals whose images are recorded.

**Example:** A member of the public requests CCTV footage of a car park, which shows their car being damaged. They say they need it so that they or their insurance company can take legal action. You should consider whether their request is genuine and whether there is any risk to the safety of other people involved.

- Are arrangements in place to restrict disclosure of images in a way consistent with the purpose for establishing the system?
- Do those that may handle requests for disclosure have clear guidance on the circumstances in which it is appropriate to make a disclosure and when it is not?
- Do you record the date of the disclosure along with details of who the images have been provided to (the name of the person and the organisation they represent) and why they are required?

Judgements about disclosure should be made by the organisation operating the CCTV system. They have discretion to refuse any request for information unless there is an overriding legal obligation such as a court order or information access rights[7]. Once you have disclosed an image to another body, such as the police, then they become the data controller for their copy of that image. It is their responsibility to comply with the Data Protection Act (DPA) in relation to any further disclosures.

The method of disclosing images should be secure to ensure they are only seen by the intended recipient.

## 8.3 Retention

The DPA does not prescribe any specific minimum or maximum retention periods which apply to all systems or footage. Rather, retention should reflect the organisation's own purposes for recording images.

You should not keep images for longer than strictly necessary to meet your own purposes for recording them. On occasion, you may need to retain images for a longer period, where a law enforcement body is investigating a crime, to give them opportunity to view the images as part of an active investigation.

**Example:** A system installed to prevent fraud being carried out at an ATM may need to retain images for several weeks, since a suspicious transaction may not come to light until the victim gets a bank statement.

**Example:** Images from a town centre system may need to be retained for enough time to allow crimes to come to light, for example, a month. The exact period should be the shortest possible, based on your own experience.

**Example:** A small system in a pub may only need to retain images for a shorter period of time because incidents will come to light very quickly. However, if a crime has been reported to the police, you should retain the images until the police have time to collect them.

- Have you decided on the shortest period that you need to retain the images, based upon your own purpose for recording the images?
- Is your image retention policy documented and understood by those who operate the system?
- Are measures in place to ensure the permanent deletion of images through secure methods at the end of this period?
- Do you undertake systematic checks to ensure that the retention period is being complied with in practice?

---

7 More information on subject access and freedom of information requests can be found in section 9.

# 9. Responsibilities

## 9.1 Letting people know

You must let people know that they are in an area where CCTV surveillance is being carried out.

The most effective way of doing this is by using prominently placed signs at the entrance to the CCTV zone and reinforcing this with further signs inside the area. This message can also be backed up with an audio announcement, where public announcements are already used, such as in a station.

Clear and prominent signs are particularly important where the cameras themselves are very discreet, or in locations where people might not expect to be under surveillance. As a general rule, signs should be more prominent and frequent where it would otherwise be less obvious to people that they are on CCTV.

In the exceptional circumstance that audio recording is being used, this should be stated explicitly and prominently.

Signs should:

- be clearly visible and readable;
- contain details of the organisation operating the system, the purpose for using CCTV and who to contact about the scheme (where these things are not obvious to those being monitored); and
- be an appropriate size depending on context, for example, whether they are viewed by pedestrians or car drivers.

Signs do not need to say who is operating the system if this is obvious. If CCTV is installed within a shop, for example, it will be obvious that the shop is responsible. All staff should know what to do or who to contact if a member of the public makes an enquiry about the CCTV system. Systems in public spaces and shopping centres should have signs giving the name and contact details of the company, organisation or authority responsible.

**Example:** “Images are being monitored and recorded for the purposes of crime prevention and public safety. This scheme is controlled by Greentown Borough Council. For more information, call 01234 567890.”

- Do you have signs in place informing people that CCTV is in operation?
- Do your signs convey the appropriate information?

## 9.2 Subject access requests

Individuals whose images are recorded have a right to view the images of themselves and, unless they agree otherwise, to be provided with a copy of the images. This must be provided within 40 calendar days of receiving a request. You may charge a fee of up to £10 (this is the current statutory maximum set by Parliament). Those who request access must provide you with details which allow you to identify them as the subject of the images and also to locate the images on your system. You should consider:

- How will the staff involved in operating the CCTV system recognise a subject access request?
- Do you have internal procedures in place for handling subject access requests? This could include keeping a log of the requests received and how they were dealt with, in case you are challenged.

A clearly documented process will also help guide individuals through such requests. This should make it clear what an individual needs to supply. You should decide:

- What details will you need to find the images? Is it made clear whether an individual will need to supply a photograph of themselves or a description of what they were wearing at the time they believe they were caught on the system, to aid identification?
- Is it made clear whether details of the date, time and location are required?
- What fee will you charge for supplying the requested images (up to a maximum of £10) and how should it be paid? Make this clear to people making access requests.
- How will you provide an individual with copies of the images?

If images of third parties are also shown with the images of the person who has made the access request, you must consider whether you need to obscure the images of third parties. If providing these images would involve an unfair intrusion into the privacy of the third party, or cause unwarranted harm or distress, then they should be obscured. In many cases, images can be disclosed as there will not be such intrusion.

**Example:** A public space CCTV camera records people walking down the street and going about their ordinary business. Where nothing untoward has occurred, this can be released without editing out third party images.

**Example:** Images show the individual who has made the request with a group of friends, waving at a camera in the town centre. There is little expectation of privacy and the person making the request already knows their friends were there. It is likely to be fair to release the image to the requester without editing out the faces of their friends.

**Example:** Images show a waiting room in a doctor’s surgery. Individuals have a high expectation of privacy and confidentiality. Images of third parties should be redacted (blurred or removed) before release.

Where you decide that third parties should not be identifiable, then you will need to make arrangements to disguise or blur the images in question. It may be necessary to contract this work out to another organisation. Where this occurs, you will need to have a written contract with the processor which specifies exactly how the information is to be used and provides you with explicit security guarantees.

## 9.3 Freedom of information

If you are a public authority then you may receive requests under the Freedom of Information Act 2000 (FOIA) or Freedom of Information (Scotland) Act 2002 (FOISA). Public authorities should have a member of staff who is responsible for responding to freedom of information requests, and understands the authority’s responsibilities. They must respond within 20 working days from receipt of the request.

Section 40 of the FOIA and section 38 of the FOISA contain a two-part exemption relating to information about individuals. If you receive a request for CCTV footage, you should consider:

- Are the images those of the requester? If so then that information is exempt from the FOIA/FOISA. Instead this request should be treated as a data protection subject access request as explained above.
- Are the images of other people? These can be disclosed only if disclosing the information in question does not breach the data protection principles.

In practical terms, if individuals are capable of being identified from the relevant CCTV images, then it is personal information about the individual concerned. It is unlikely that this information can be disclosed in response to an FOI request as the requester could potentially use the images for any purpose and the individual concerned is unlikely to expect this. This may therefore be unfair processing in contravention of the Data Protection Act (DPA).

This is not an exhaustive guide to handling FOI requests[8].

**Note:** Even where footage is exempt from FOIA/FOISA it may be lawful to provide it on a case-by-case basis without breaching the DPA, where the reason for the request is taken into account. See section 8 (using the images) for advice on requests for disclosure.

### 9.4 Other responsibilities

Staff operating the CCTV system also need to be aware of two further rights that individuals have under the DPA. They need to recognise a request from an individual to prevent processing likely to cause substantial and unwarranted damage or distress (s10 DPA) and one to prevent automated decision-taking in relation to the individual (s12 DPA). Experience has shown that the operators of CCTV systems are highly unlikely to receive such requests. If you do, guidance on these rights is available from the Information Commissioner's Office[9]. Any use of Automatic Facial Recognition technology should also involve human intervention before decisions are taken, and this would not be decision taking solely on an automated basis within the terms of the DPA.

If the CCTV system covers a public space, the organisation operating the CCTV system should be aware of the possible licensing requirements imposed by the Security Industry Authority.

A public space surveillance (CCTV) licence is required when operatives are supplied under a contract for services. Under the provisions of the Private Security Industry Act 2001, it is a criminal offence for staff to be contracted as public space surveillance CCTV operators in England, Wales and Scotland without an SIA licence[10].

- Do the relevant staff know how to deal with any request to prevent processing or prevent automated decision making and where to seek advice?
- Have you satisfied any relevant licensing requirements?

8 Further information about the FOIA can be found on ICO's website: www.ico.gov.uk including specific guidance about section 40 (FOI Awareness Guidance No1).

9 "How can I stop them processing my personal information?" and "Preventing decisions based on automated processing of personal information" can both be found on the ICO website: www.ico.gov.uk. You may also wish to consult our Legal Guidance.

10 This requirement does not apply in Northern Ireland. For more information visit www.the-sia.org.uk

# 10. Staying in control

Once you have followed the guidance in this code and set up the CCTV system you need to ensure that it continues to comply with the Data Protection Act (DPA) and the code's requirements in practice. If requested you should:

- tell people how they can make a subject access request, who it should be sent to and what information needs to be supplied with their request;
- give them a copy of this code or details of the Information Commissioner's Office (ICO) website; and
- tell them how to complain about either the operation of the system or failure to comply with the requirements of this code.

Staff using the CCTV system or images should be trained to ensure they comply with this code. In particular, do they know:

- what the organisation's policies are for recording and retaining images?
- how to handle the images securely?
- what to do if they receive a request for images, for example, from the police?
- how to recognise a subject access request and what to do if they receive one?

All images must be protected by sufficient security to ensure they do not fall into the wrong hands. This should include technical, organisational and physical security. For example:

- Are sufficient safeguards in place to protect wireless transmission systems from interception?
- Is the ability to make copies of images restricted to appropriate staff?
- Where copies of images are disclosed, how are they safely delivered to the intended recipient?
- Are control rooms and rooms where images are stored secure?
- Are staff trained in security procedures and are there sanctions against staff who misuse CCTV images?
- Are staff aware that they could be committing a criminal offence if they misuse CCTV images?

Any documented procedures which you produce following on from this code should be reviewed regularly, either by a designated individual within the organisation or by a third party. This is to ensure the standards established during the setup of the system are maintained.

Similarly, there should be a periodic review (at least annually) of the system's effectiveness to ensure that it is still doing what it was intended to do. If it does not achieve its purpose, it should be stopped or modified.

- Is information available to help deal with queries about the operation of the system and how individuals may make access requests?
- Does the information include your commitment to the recommendations in this code and include details of the ICO if individuals have data protection compliance concerns?
- Is a system of regular compliance reviews in place, including compliance with the provisions of this code, continued operational effectiveness and whether the system continues to meet its purposes and remains justified?
- Are the results of the review recorded, and are its conclusions acted upon?

# Appendix 1

### The Data Protection Act 1998: data protection principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-

   (a) at least one of the conditions in Schedule 2 is met, and

   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

This is not a full explanation of the principles. For more general information, see our Legal Guidance[1].

---

1 The ICO's "Data Protection Act 1998 Legal Guidance" is available on the ICO website: www.ico.gov.uk.

# Appendix 2

### Checklist for users of limited CCTV systems monitoring small retail and business premises

This CCTV system and the images produced by it are controlled by …….. who is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose (which is a legal requirement of the Data Protection Act 1998)[1].

We (……) have considered the need for using CCTV and have decided it is required for the prevention and detection of crime and for protecting the safety of customers. It will not be used for other purposes. We conduct an annual review of our use of CCTV.

| | Checked (Date) | By | Date of next review |
|---|---|---|---|
| Notification has been submitted to the Information Commissioner and the next renewal date recorded. | | | |
| There is a named individual who is responsible for the operation of the system. | | | |
| A system has been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required. | | | |
| Cameras have been sited so that they provide clear images. | | | |

| | | | |
|---|---|---|---|
| Cameras have been positioned to avoid capturing the images of persons not visiting the premises. | | | |
| There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s). | | | |
| Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them. | | | |
| The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated. | | | |
| Except for law enforcement bodies, images will not be provided to third parties. | | | |
| The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made. | | | |
| Regular checks are carried out to ensure that the system is working properly and produces high quality images. | | | |

**Please keep this checklist in a safe place until the date of the next review.**

---

1 Not all small businesses need to notify. Current notification requirements can be found at www.ico.gov.uk/what_we_cover/data_protection/notification.aspx

# Appendix 3

### Monitoring your workforce

When you install CCTV in a workplace, such as a shop, it is likely to capture pictures of workers, even if they are not the main subject of surveillance. If the purpose of the CCTV is solely to prevent and detect crime, then you should not use it for monitoring the amount of work done or compliance with company procedures.

- Have the cameras been installed so they are not directed specifically to capture images of workers?
- Are the recorded images viewed only when there is suspected criminal activity, and not just for routine monitoring of workers? Cameras installed for preventing and detecting crime should not be used for non-criminal matters.
- Are images of workers used only if you see something you cannot be expected to ignore, such as criminal activity, gross misconduct, or behaviour which puts others at risk?
- If these images are used in disciplinary proceedings, is the footage retained so that the worker can see it and respond? A still image is unlikely to be enough.

In some cases, it may be appropriate to install CCTV specifically for workforce monitoring. You should go through the decision making process in section 4 of this code and consider whether it is justified. In particular, consider whether better training or greater supervision would be a more appropriate solution.

**Example:** You suspect that your workers are stealing goods from the store room. It would be appropriate to install CCTV in this room, as it will not involve continuous or intrusive monitoring and is proportionate to the problem.

**Example:** You suspect that your workers are making mobile phone calls during working hours, against company policy, and you consider installing CCTV cameras on their desks to monitor them throughout the day. This would be intrusive and disproportionate. Continuous monitoring should only be used in very exceptional circumstances, for example where hazardous substances are used and failure to follow procedures would pose a serious risk to life.

- Is CCTV limited to areas which workers would not expect to be private? CCTV should not be used in toilet areas or private offices.
- Are workers made aware that the CCTV is for staff monitoring and how it will be used? How are visitors informed that CCTV is in operation?
- If CCTV is used to enforce internal policies, are workers fully aware of these policies and have they had sufficient training?
- Do you have procedures to deal appropriately with subject access requests from workers?

Workers should normally be aware that they are being monitored, but in exceptional circumstances, covert monitoring may be used as part of a specific investigation. Covert monitoring is where video or audio recording equipment is used, and those being monitored are unaware that this is taking place. Before approving covert monitoring, you should ask yourself:

- Is this an exceptional circumstance, and is there is reason to suspect criminal activity or equivalent malpractice?
- Will the cameras only be used for a specific investigation, and will they be removed once the investigation is complete?
- Would it prejudice the investigation to tell workers that cameras are being used?
- Have you taken into account the intrusion on innocent workers?
- Has the decision been taken by senior management?

Cameras and listening devices should not be installed in private areas such as toilets and private offices, except in the most exceptional circumstances where serious crime is suspected. This should only happen where there is an intention to involve the police, not where it is a purely internal disciplinary matter.

In some cases, covert cameras installed for one investigation may turn up evidence of other criminal behaviour or disciplinary offences. You should only make use of this where the offence is serious, for example, gross misconduct or misconduct putting others at risk. It would be unfair to use evidence obtained covertly for minor disciplinary matters.

In some cases, covert monitoring may be covered by the Regulation of Investigatory Powers Act 2000 or the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPA / RIPSA). You may wish to seek advice[1].

More advice on monitoring workers can be found in our Employment practices code[2].

If you would like to contact us please call 08456 306060, or 01625 545745 if you would prefer to call a national rate number.

e:mail@ico.gsi.gov.uk

January 2008

---

1 The Home Office guidance on RIPA can be found at http://security.homeoffice.gov.uk/ripa

2 The Employment practices code and other related guidance can be found on the ICO website: www.ico.gov.uk.