Data Protection

CCTV code of practice

Draft for consultation
20 May 2014 – 1 July 2014

ico.
Information Commissioner's Office

Contents

1. Foreword

To be added post consultation

2. About this code

This code provides good practice advice for those involved in operating CCTV and other surveillance camera devices that view or record individual's information, and covers other information that relates to individuals (for example vehicle registration marks captured by Automatic Number Plate Recognition - ANPR equipment). This code uses the terms 'surveillance system(s)', 'CCTV' and 'information' 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 organisations 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 access their personal information, 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 they risk breaking the law.

This code also reflects the wider regulatory environment. When using, or intending to use surveillance systems, many organisations also need to consider their obligations in relation to the Freedom of Information Act 2000 (FOIA), the Protection of Freedoms Act 2012 (PFA), the Human Rights Act 1998 (HRA) and the Secretary of State's Surveillance Camera Code of Practice (SC code). The ICO's code also reflects recent case law in relation to surveillance systems.

This code is consistent with the SC code and therefore following the guidance contained in this document will also help you comply with many of the principles in that code. The SC code explains that it:

> *'...provides guidance on the appropriate and effective use of surveillance camera systems by relevant authorities...'*

The PFA allows for relevant authorities to be designated and these are currently Police Forces, Police and Crime Commissioners and Local Authorities in England and Wales. Further details are available here: www.gov.uk - Surveillance Camera Commissioner.

The CCTV code of practice has a greater coverage than the SC code as the DPA is applicable to all organisations that process personal data irrespective of sector and across the whole of the UK. Any organisation

using cameras to process personal data should follow the recommendations of this code.

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

Following the recommendations in this code will:

- help ensure that those capturing individuals' information comply with the DPA and other relevant statutory obligations;
- contribute to the efficient deployment and operation of a camera system;
- mean that the information captured is usable and can meet its objectives in practice;
- reduce reputational risks by staying within the law and avoiding regulatory action and penalties;
- re-assure those whose information is being captured;
- help inspire wider public trust and confidence in the use of CCTV; and
- help relevant authorities to comply with the SC code.

This code replaces the earlier code of practice issued by the Information Commissioner's Office (ICO) in 2008 and the supplementary compliance checklist. It takes account of the technical, operational and legal changes that have taken place since the last review of the code and the lessons learned from enforcement action.

3. What this code covers

The majority of surveillance systems are used to monitor and/or record the activities of individuals. As such they process individuals' information - their personal data. Most uses of surveillance systems will therefore be covered by the DPA and the provisions of the code, whether the system is used by a multinational company to monitor entry of staff and visitors in and out of its premises, or a local newsagent recording information to help prevent crime.

- This code also covers the use of camera related surveillance equipment such as Automatic Number Plate Recognition (ANPR), body worn video cameras (BWV), remotely operated vehicles (drones), and other systems that capture information of identifiable individuals or information relating to individuals.

This code also provides guidance on information governance requirements, such as data retention and disposal, which it is important to follow in order to comply with the data protection principles.

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

> **Example:** A video of your child in a nativity play recorded for your own family use is not covered by the DPA.

This code is primarily aimed at businesses and organisations that routinely capture individuals' information on their surveillance systems. 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 public authorities 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. This type of recording is covert and directed at an individual or individuals[1].

> **Example:** The police monitoring and recording the movement of a suspected drug dealer with covert surveillance equipment to identify whether they are committing any related offences.

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 an exemption within the DPA applies to such activities that are carried out for journalistic, artistic and literary purposes. This code does however apply to the passing on of surveillance system information to the media.

Not all sections of the code will be fully relevant to all surveillance systems; this will depend upon the extent and use of the information. Although small-scale users (such as small retailers) are covered by the DPA, they are unlikely to have sophisticated systems, so many of this

[1] For further information please refer to the following: https://www.gov.uk/surveillance-and-counter-terrorism and the Surveillance Road Map.

code's more detailed provisions will be inappropriate. Appendix 2 provides special guidance, as an alternative to the full code, for very limited use of surveillance systems where privacy risks are small and resources are limited. If you are a small scale user, but you wish to use your surveillance system for any purpose which is not covered in the checklist, you should read the full code.

Note: The DPA applies to information captured by surveillance systems. This code does not cover the use of dummy or non-operational systems. However, it would cover the piloting of live systems as personal data will be captured.

4. Deciding when surveillance camera systems should be used

Using surveillance systems can be privacy intrusive. They are capable of placing large numbers of law-abiding people under surveillance and recording their movements as they go about their day to day activities. As such, you should carefully consider whether or not to use a surveillance system. The fact that it is possible, affordable or has public support should not be the primary motivating factor. You should also take into account the nature of the problem you are seeking to address; whether a surveillance system would be a justified and effective solution, whether better solutions exist, what effect its use may have on individuals, and whether in the light of this, its use is a proportionate response to the problem. If you are already using a surveillance system, you should evaluate whether it is necessary and proportionate to continue using it.

> **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. The best way to do this is to conduct a privacy impact assessment (PIA). The ICO has produced a code of practice explaining how to go about this, 'Conducting privacy impact assessments code of practice'.

A privacy impact assessment looks at privacy in a wider context than just the DPA, it also takes into consideration the HRA (where the data controller is also a public authority), and the impact on privacy rights. It should look at what pressing need the surveillance system is supposed to address, and show whether or not the system will meet this need, based

on reliable information and whether the surveillance system proposed can be justified as proportionate to the needs identified.

Note: Although private companies are not subject to the HRA, in conducting a PIA and an evaluation of proportionality and necessity, you will be looking at concepts that would also impact upon fairness under the first data protection principle. Private sector organisations should therefore also consider these issues.

A PIA should look at the pressing need that the surveillance system is intended to address and whether its proposed use has a lawful basis and is justified, necessary and proportionate. Where the system is already in use, the same issues should be considered or considerations should be made as to whether a less privacy intrusive method could be used to address the pressing need. Guiding Principle 1 of the SC echoes what is said in this section.

> **Example:** A police force could use a temporary or vehicle based mobile ANPR car to help it decide if it addresses the pressing need in a particular location before establishing a permanent system.

Failure to carry out an approriate PIA in advance has contributed to many of the data protection problems that have occurred in relation to the use of surveillance systems, for example, the 'Royston ring of steel' in which the ICO issued an enforcement notice to Hertfordshire Constabulary.

5. Governance

5.1 Ensuring effective administration

Establishing a clear basis for the processing of any personal information is essential, and the handling of information relating to individuals collected from surveillance systems is no different. It is important to establish who has responsibility for the control of this information, for example, deciding what is to be recorded, how the information should be used and to whom it may be disclosed. The organisation that makes these decisions is called the data controller and is legally responsible for compliance with the DPA.

Relevant authorities under the PFA should also take note of Guiding Principle 4 of the SC code.

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 information and making decisions about how it 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 ICO that they are the data controller? Does the notification cover the purposes for which the information is used, the disclosures that are made, and other relevant details?[2]
- If someone outside your organisation provides you with any processing services, for example editing information (such as CCTV images), is a written contract in place with clearly defined responsibilities? This should ensure that information is 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.

Example: Public authorities may share a common control room for a surveillance system in order to cut back on running costs. If the surveillance system monitors the inside of a hospital but also monitors the high street, then different privacy expectations will apply to the information gained from each. The agreement to share services must have guidelines and procedures in place to ensure that control and use of these systems is appropriate and staff must be appropriately trained to deal with the differing levels of sensitivity of information. It should also be made clear who is in control of what information in a shared service situation such as this.

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 information, and have these been communicated to those who operate the system?
- Are there clearly documented procedures, based on this code, for how information should be handled in practice? This could include

[2] 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.org.uk/what_we_cover/data_protection/notification.aspx

guidance on disclosures and how to keep a record of these. Have these been given to the 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 that the system complies with this code and 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.

Relevant authorities should take note of Guiding Principle 5 of the SC code.

You should regularly review whether the use of surveillance systems continues to be justified. It is necessary to renew your notification with the ICO yearly, so this would be an appropriate time to consider the ongoing use of such systems.

You should also take into account other relevant rules and guidance which may cover your activities. For example the ICO's 'Privacy notices code of practice', 'Data sharing code of practice', 'Employment practices code', 'Employment practices code - supplementary guidance' (this supplementary guidance is particularly important if surveillance systems will be used to monitor employees) and as mentioned above the 'Conducting privacy impact assessments code of practice'.

5.2 Looking after the recorded material and using the information

5.2.1 Storing and viewing surveillance system information

Recorded material should be stored in a way that maintains the integrity of the information. This is to ensure that the rights of individuals recorded by surveillance systems are protected and that the information can be used as evidence in court. To do this you need to carefully choose how the information is held and recorded, and ensure that access is restricted. You will also need to ensure that the information is secure and where necessary, encrypted. You may wish to keep a record/audit trail of how the information is handled if it is likely to be used as evidence in court. Finally, once there is no reason to retain the recorded information, it should be deleted. Exactly when you decide to do this will depend on the purpose for using the surveillance systems. A record/audit trail of this should also be captured.

Many modern surveillance 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 information can be used by appropriate law enforcement agencies if this is envisaged. If they cannot, this may undermine the purpose for undertaking surveillance. Relevant authorities under PFA should also take note of Guiding Principle 9 of the SC.

- How practicable 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?
- Can it be provided in a suitable format?
- How can you ensure that information complies with a designated standard?
- Will they find your recorded information 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, ie out of sight of the reception area. They should be positioned 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.

Where images are in an area of particular sensitivity such as a changing room, it may be more appropriate to only view recorded images after an incident has occurred.

- 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?
- Does real time monitoring need to take place?

5.2.2 Disclosure

Disclosure of information from surveillance systems must also be controlled and consistent with the purpose(s) for which the system was established. For example, it can be appropriate to disclose surveillance information to a law enforcement agency when the purpose of the system is to prevent and detect crime, but it would not be appropriate to place them on the internet. It may also not be appropriate to disclose information about identifiable individuals to the media. Placing such information on the internet incorrectly or without full consideration of what is being done may cause the disclosure of individuals' personal data and sensitive personal data. In severe cases, this may lead to the ICO taking enforcement action. Information can be released to the media for identification purposes; this should not generally be done by anyone other than a law enforcement agency.

Note should also be taken of Guiding Principle 7 of the SC by relevant authorities under the PFA.

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

Any other requests for information should be approached with care as wider disclosure may be unfair to the individuals concerned. In some limited circumstances it may be appropriate to release information to a third party, where their needs outweigh those of the individuals whose information is 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 information 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 information has been provided to (the name of the person and the organisation they represent) and why they are required?

When disclosing surveillance images of individuals, consideration needs to be given to whether or not obscuring of identifying features is necessary. Whether or not it is necessary to obscure will depend on the nature and context of the footage that is being considered for disclosure.

> **Example:** if footage from a camera that covers the entrance to a drug rehabilitation centre is held, then consider obscuring the images of people entering and leaving it as this could be considered sensitive personal data. This may involve an unfair intrusion into the privacy of the individuals whose information is captured and may cause unwarranted harm or distress. On the other hand, footage of individual's entering and exiting a bookshop is far less likely to require obscuring.

It may be necessary to contract obscuring 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.

Judgements about disclosure should be made by the organisation operating the surveillance 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 (see sections 5.2.3 and 5.2.4). Once you have disclosed information to another body, such as the police, they become the data controller for the copy they hold. It is their responsibility to comply with the DPA in relation to any further disclosures.

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

5.2.3 Subject access requests

Individuals whose information is recorded have a right to view this information and unless they agree otherwise, to be provided with a copy of that information. This must be provided promptly and within no longer than 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 information and also to locate the information on your system. You should consider:

- How staff involved in operating the surveillance system will recognise a subject access request.
- Whether internal procedures for handling subject access requests are in place. 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 consider:

- The details you will need to find the information. 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.
- If not a CCTV system, the information they need to provide, eg. their vehicle registration mark (VRM) in relation to ANPR information.
- If details of the date, time and location are required.
- The fee you will charge for supplying the requested information (up to a maximum of £10) and how should it be paid. Make this clear to people making access requests.
- If you have effectively labelled information to assist with retrieval.
- How you will provide an individual with copies of the information held.

As mentioned in 5.2.2 where information of third parties is also shown with the information of the person who has made the access request, you must consider whether you need to obscure this information taking into account the considerations discussed in 5.2.2.

For further information on subject access requests, please refer to the ICO's 'Subject access code of practice'.

5.2.4 Freedom of information

If you are a public authority then you may receive requests under the 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 surveillance system information, you should consider:

- Is the information personal data 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.
- Is the information personal data of other people? If so it can only be disclosed if this would not breach the data protection principles.

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

However, consideration can be made of the expectations of the individuals involved, what the information considered for disclosure would reveal and the legitimate public interest in the information when deciding on whether disclosure is appropriate.

Where you think obscuring images will appropriately anonymise third party personal data, ie it is reasonably likely that the requestor or anyone else can identify the individuals whose personal data you wish to protect (disclosure under FOIA being disclosure to the world), then it may be appropriate to do this rather than exempting the information.

If you are a public authority who has surveillance systems, you may also receive requests for information under FOIA relating to those surveillance systems. For example, requestors may ask for information regarding the operation of the systems, the siting of them, or the costs of using and maintaining them.

If this is information which is held, then consideration will need to be given to whether or not it is appropriate to disclose this information under FOIA. If it is not appropriate to disclose this information then an exemption under FOIA will need to be used, if one is applicable.[3]

[3] It is worth noting that the Upper Tribunal (remitted to the First-tier Tribunal) judgement in Mathieson v IC and Chief Constable of Devon and Cornwall, ruled the location of ANPR cameras did not have to be disclosed in relation to a request for information under FOIA where to do so would impact upon national security or the prevention or detection of crime.

This is not an exhaustive guide to handling FOI requests[4].

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 5.2.2 above for advice on requests for disclosure.

5.2.5 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 information. The retention period should be informed by the purpose for which the information is collected and how long it is needed to achieve this purpose. It should not be kept for longer than necessary or because the system manufacturer's information tells you how long information can be held for.

> **Example:** Footage from a surveillance system shouldn't be kept for five weeks merely because the manufacturer's settings on the surveillance system allow retention for this length of time.

Where it is not necessary to retain information, for example, it does not achieve the purpose for which you are collecting and retaining information, then it should be deleted.

> **Example:** If a supermarket uses an ANPR system to monitor use of its car park when there is a 2 hour free parking limit and retains the details gathered from the ANPR system for those cars that have not exceeded the parking limit, then this is unnecessary and excessive and unlikely to comply with the data protection principles. (In this example the vehicle registration mark (VRM) is an individual's personal data).

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

[4] For further information on FOIA, including how to handle requests for information, please refer to the ICO's 'Guide to Freedom of Information'.

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 information, based upon your own purpose for recording it?
- Is your information retention policy documented and understood by those who operate the system?
- Are measures in place to ensure the permanent deletion of information 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?

Relevant authorities should take note of Guiding Principle 6 of the SC code.

5.3 Staying in control

Once you have followed the guidance in this code and set up the surveillance system you need to ensure that it continues to comply with the DPA and the code's requirements in practice. 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 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 surveillance system or information 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 information?
- How to handle the information securely?
- What to do if they receive a request for information, for example, from the police?
- How to recognise a subject access request and what to do if they receive one?

All information must be sufficiently protected to ensure that it does 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 information restricted to appropriate staff?
- Are there sufficient controls and safeguards in place if the system is connected to or available across an organisational network or intranet?
- Where information is disclosed, how is it safely delivered to the intended recipient?
- Are control rooms and rooms where information is stored secure?
- Are staff trained in security procedures and are there sanctions against staff who misuse surveillance system information?
- Are staff aware that they could be committing a criminal offence if they misuse surveillance system information?

Any documented procedures that you produce following on from this code should be regularly reviewed, 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 it addressing the needs and delivering the benefits that justified its use?
- 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?

Attention should also be paid to Guiding Principle 10 of the SC code by relevant authorities under the PFA.

> **Example:** A CCTV system implemented to deal with persistent problems of nightlife related incidents may no longer be justified if the location of the nightlife district has migrated to another area of town over the intervening years.

6. Selecting and siting surveillance systems

Any surveillance system information must be adequate for the purpose for which you are collecting it. It is essential that you choose surveillance systems and locations that achieve the purposes for which you are using it.

As outlined earlier in this code, you should identify, through a privacy impact assessment, whether or not a surveillance system is the most appropriate means of addressing the pressing need. If having decided this is the case, a privacy by design approach should be considered when making decisions about which equipment to purchase, see section 7.4 for more details. You should look to identify which equipment will address the pressing need but is also restricted so that it does no more than is necessary for its specified purpose.

> **Example:** A CCTV system that allows recording to be switched on and off easily, and therefore does not have to record continuously, will help mitigate the potential risk of recording excessive information.

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 unnecessary images

are not viewed or recorded, and those that are recorded 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 and that appropriate restrictions on viewing and disclosing images are in place.

To judge the necessary quality of images, you will need to take into account the purpose for which CCTV is used and the level of quality required to achieve the purpose. Guiding principle 8 of the SC code provides clear and practical advice on how to identify the needs of a surveillance system. The ICO would recommend and expect you to comply with the same standards as recommended in this principle.

7. Examples of emerging technologies

Surveillance systems have advanced greatly since the last version of this code was published. This section takes a look at a few of the more

prevalent current technologies and provides an oversight as to how to approach them. The body of this code will also be relevant to these technologies. However, they present novel issues that it is worth looking at separately.

7.1 ANPR systems

The capabilities of ANPR systems and their use have increased since the last revision of this code. The level of data collected, analysed and used, the increased ease with which ANPR systems can now be linked to other systems (and the potential risks under the DPA this may pose), the increasing affordability of these systems, and its increased use in both the public and private sector means that it is a technology that requires particular attention.

- Is the system just recording vehicle registration marks or images of vehicles/occupants or 'patch plates' as well, if so why is this justified?
- Has a PIA been undertaken which reflects the mass acquisition of details that are capable of tracking many individuals' movements?
- Are underlying matching databases of the right quality and kept up to date?
- Are retention periods the minimum necessary for the purpose, such as ensuring deletion where parking restrictions are complied with?
- Are adequate measures in place to warn individuals of mobile or vehicle based ANPR?

7.2 Body worn video cameras

BWVs are cameras that are worn on a person, usually attached to their clothing or uniform. They can record visual and audio information. The reducing cost of this type of equipment means that smaller businesses and the public are increasingly able to purchase and use such equipment, alongside larger organisations, such as law enforcement agencies.

- Is the device only turned on to record when an incident occurs or is it continuous? If it is continuous, and particularly where audio is also recorded, is this justified?
- Has a sufficiently detailed PIA been conducted which includes the evaluation of the justification of the use of BWVs, as opposed to less privacy intrusive alternatives?
- Is there adequate fair processing information provided to individuals who may be recorded? For example, do individuals wearing the BWV have signage on their uniform alerting individuals to the recording? Can additional information be made available on the organisation's website?

- Have appropriate technical security restrictions been put in place to protect the recorded information?
- Are retention periods the minimum necessary for the purpose?
- Is there a data sharing agreement in place if recorded information is routinely shared with third parties?

Example: It may be appropriate for a Parking Enforcement Officer to switch on their BWV where they believe an individual is being aggressive or there is the potential for aggression. However, it would not be appropriate to switch it on where an individual is merely asking for directions.

7.3 Remotely operated vehicles (Drones)

Drones are unmanned vehicles which are capable of visual recording whilst airborne, they can vary in size from the very large (the size of a plane) to the very small (the size of a remote control plane/helicopter). They have developed from military use initially but are now much more affordable and as with BWVs, the smaller devices can be easily purchased by businesses and members of the public.

Example: A business may purchase a drone to monitor inaccessible areas such as a roof to check for damage. Its use should be limited to that specific function and recording should not occur when flying over other areas that may capture images of individuals.

- Has a PIA been undertaken which justifies the drone's use, rather than a less privacy intrusive method?
- Has a method of informing individuals that recording is taking place been identified? Has a method of providing fair processing information been identified?
- Is the recording continuous or triggered by something? If recording is continuous, is it proportionate and justifiable?
- Is there a method by which recording can be restricted to the focus of the drones attention, rather than recording a wide field of vision?
- Have appropriate security measures, such as encryption and access controls been put in place?
- Have appropriate retention and deletion schedules been incorporated?[5]

[5] For more useful information, please look at this briefing note produced by the Information & Privacy Commissioner Ontario, Canada

7.4 Privacy impact assessments and privacy by design

Clearly all of these emerging technologies have the potential to be privacy intrusive. None of these devices should be purchased merely because they are available, affordable or in the belief that it will garner public approval.

It is therefore very important that you perform a PIA. As mentioned earlier in this document, the ICO has produced a code of practice which can help you do this, 'Conducting privacy impact assessments code of practice'. You will need to consider the privacy issues involved with using these new surveillance systems and see if their use would be necessary and proportionate and address a pressing need that you have identified. You should consider less privacy intrusive methods of achieving this need where possible. PIAs are also beneficial because consultation is a key element of the process; this enables an insight into the public reaction and views about potential privacy intrusion.

If using these devices, you should incorporate privacy by design features. This should be in your criteria for procuring the device and in the decisions you make about deployment and configuration. For example, making sure the equipment has the ability to be switched on or off, if this is appropriate, so that recording is not continuous. Unless continuous recording can be shown to be justified, you should only record where it is necessary and is done for the purpose for which its use is specified. The equipment must obviously also be of sufficient quality and standard to achieve its stated purpose.

> **Example**: A car park operator is looking at whether to use ANPR to enforce parking restrictions. A PIA is undertaken which identifies how ANPR will address the problem, the privacy intrusions and the ways to minimise these intrusions, such as information being automatically deleted when a car that has not contravened the restrictions leaves a car park.

7.5 Privacy notices

It is clear that these and similar devices present more difficult challenges in relation to providing individuals with fair processing information, something which is a requirement following the first principle of the DPA. Clearly it will be difficult to provide an individual with this information when the surveillance system is airborne, or on a person or in the case of ANPR, not visible at ground level or more prevalent then it may first appear.

However, these are issues that must be tackled as you are unlikely to comply with the data protection principles if you do not provide an appropriate notice. If you are considering using such devices, you will need to come up with appropriate and potentially innovative ways of informing individuals of their rights.

> **Example:** If a drone is to be operating in a specific area at a specific time then it may be that the organisation operating the drone can use social media to promote the usage and provide a link to the related privacy notice and any other relevant information.

One of the main rights that a privacy notice explains is an individual's right of subject access. If you have decided that you are going to use these devices you will need to have the ability to provide information to requestors, be able to obscure or edit the information where necessary and have staff trained who are able to deal with all the facets of subject access. Consideration will also need to be made regarding requests for information under FOIA.

8. Using the equipment

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

- Does your recording system produce good clear quality information? Will the quality of the information be maintained throughout 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 information cannot be inadvertently corrupted?
- Is there a regular check that the date and time stamp recorded on images is accurate?
- If automatic recognition technology is being used such as facial recognition or gait recognition (the identification of individuals by the unique way in which they walk), is the matching effective in practice, is the surveillance system placed so that facial images or images of the individual moving 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 information?
- Have you ensured that your wireless transmission system is suitably secure, if one is used? If necessary, do you have the ability to encrypt information?
- As with ANPR systems where existing matching databases are used, have you ensured their accuracy? Do you have procedures in place for the continued monitoring of databases accuracy? Relevant authorities under the PFA should also take note of Guiding Principle 12 of the SC code.

Surveillance systems should 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, unless you can clearly justify its use with clear supporting evidence.

> **Example:** Where you are considering using an audio capability on a BWV system, have you considered whether this is appropriate in a PIA and if so, have you mitigated the level of intrusion by using privacy by design?

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.
- Where recording is triggered due to a specific threat.

This advice reflects the decision in the case involving Southampton City Council (the council) in which the ICO issued an enforcement notice to the council ordering it to stop making it a requirement of gaining a taxi license to have continuous video and audio recording in taxis. The ICO and ultimately the First-Tier Tribunal (Information Rights) considered this to be a breach of principle one of the DPA, it being disproportionate and not justified under article 8 of the HRA (the right to private life). It was therefore considered unlawful under the first principle of the DPA. The

argument above would similarly apply to other forms of public transport, unless clear justification for continuous recording can be evidenced.

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 and its use is not well justified 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?

9. Responsibilities

9.1 Letting people know

You must let people know that they are in an area where a surveillance system is being operated.

The most effective way of doing this is by using prominently placed signs at the entrance to the surveillance system's 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 on a train.

Clear and prominent signs are particularly important where the surveillance systems 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 being monitored by a surveillance system. This may be particularly important when an ANPR system covering a large area is being used.

In the exceptional circumstance that audio recording is being used, this should be stated explicitly and prominently. It should also be clearly stated if audio recording is used for a different or further purpose than visual recording.

Signs should:

- be clearly visible and readable;
- contain details of the organisation operating the system, the purpose for using the surveillance system and who to contact about the scheme (where these things are not obvious to those being monitored);
- include basic contact details such as simple website address, telephone number or email contact; 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 a surveillance system 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 surveillance 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?

If you are a relevant authority under the PFA you must take note of Guiding Principle 3 with regards to transparency.

It is also recommended in most FOIA publication scheme definition documents that the location of CCTV systems should be published.

9.1.2 Signs on roads

It is important that if cameras are used on the road network or in areas that vehicles have access, like car parks, there are appropriate signs to alert drivers to the use of cameras. It is also important that these signs do not affect the safety of road users. This could limit the information conveyed particularly where the road has a high speed limit. Signs must make clear that cameras are in use and who is operating them so that individuals know who holds information about them and therefore have the opportunity to make further enquires about what is happening to the

personal information about them. Where authorised signs under road traffic sign regulations are used and these do not convey the details of the organisation then supplementary signs should be used such as those permitted by Town and Country Planning (control of advertisements) Regulations 2007.

9.2 Other responsibilities

Staff operating a surveillance 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 surveillance systems are highly unlikely to receive such requests. If you do, guidance on these rights is available from the Information Commissioner's Office.[6] Any use of Automatic Face or Gait Recognition technology should also involve human intervention before decisions are taken, and should not be a decision made solely on an automated basis within the terms of the DPA.

If the surveillance system covers a public space, the organisation operating the 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.[7]

- 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?

[6] "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.org.uk. You may also wish to consult our Legal Guidance.
[7] This requirement does not apply in Northern Ireland. For more information visit www.the-sia.org.uk

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.org.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.			
The problem we are trying to address has been clearly defined and installing cameras is the best solution.			
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 potential impact on individuals' privacy has been identified and taken into account in the use of the system.			
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.org.uk/what_we_cover/data_protection/notification.aspx