KESGRAVE TOWN COUNCIL

Data Protection Policy (Use of CCTV)

1. Background

1.1 Council uses closed circuit television (CCTV) images for the prevention, identification and reduction of crime and monitoring of its property in order to provide a safe and secure environment for staff and residents and to prevent the loss or damage to Council property.

1.2 CCTV surveillance is intended for the purposes of:

- protecting Council's assets;
- promoting the health and safety of staff and residents;
- reducing the incidence of crime and anti-social behaviour (including vandalism);
- supporting the Police in a bid to deter and detect crime; and
- assisting in identifying, apprehending and prosecuting offenders.

1.3 The system comprises of 4 fixed cameras positioned at the Multi-Use Games Area located at Cedarwalk Green, Kesgrave (the "MUGA").

1.4 The CCTV system is owned and operated by Council and the deployment of which is determined by Council through the Clerk.

1.5 The CCTV is not continuously monitored. Data/images are accessed upon receipt of reports of potential criminal or anti-social behaviour.

1.6 The CCTV Scheme is registered with the Information Commissioner under the terms of the Data Protection Act. This Policy outlines Council's use of CCTV and how it complies with the Act.

1.7 All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. All operators are trained in their responsibilities under the Information Commissioner's Office (ICO) CCTV Code of Practice appended to this policy. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images.

1.8 Council complies with the ICO CCTV Code of Practice appended to this policy to ensure its CCTV system is used responsibly and safeguards both trust and confidence in its continued use.

1.9 The use of the CCTV system will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies for other purposes is prohibited by this Policy e.g. CCTV will not be used for monitoring employee performance.

1.10 CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by Council, including its Complaints Policy and Procedure.

2. Justification for Use of CCTV

The use of CCTV to monitor the MUGA for security purposes has been deemed to be justified by Council. The system is intended to capture images of individuals damaging or misusing property or any anti-social behaviour within or close to the MUGA.

3. Data Protection Impact Assessments

Where new CCTV systems or cameras are to be installed, Council will carry out a full Data Protection Impact Assessment identifying risks related to the installation and ensuring full compliance with data protection legislation. This may involve the need for consultation with staff and local residents.

4. Location of Cameras

4.1 Cameras will be sited so they only capture images relevant to the purposes for which they are installed and care will be taken to ensure that reasonable privacy expectations are not violated.

4.2 Council will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act.

4.3 CCTV will not be used within Council premises.

4.4 Cameras placed so as to record external areas are positioned in such a way as to prevent or minimise recording of passers-by.

4.5 CCTV Video Monitoring and Recording of Public Areas may include the following:

- protection of Council property: building perimeters, entrances and exits; and
- criminal investigations (carried out by the Police): robbery, burglary and theft surveillance.

5. Covert Surveillance

Council will not engage in covert surveillance.

6. Notification

6.1 A copy of this CCTV Policy will be provided on request to staff or residents and will be made available on Council's website.

6.2 The location of CCTV cameras will also be indicated and adequate signage will be placed at each location in which a CCTV camera is sited to indicate that CCTV is in operation. Appropriate locations for signage will include:

- at entrances to premises i.e. external doors, gates; and
- at or close to each camera.

7. Storage and Retention

7.1 The images captured by the CCTV system will be retained for a maximum of 30 days, except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue and will be destroyed within six months of its final conclusion.

7.2 The images/recordings will be stored in a secure environment with a log of access kept.

7.3 Access will be restricted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of the Clerk. The Clerk may delegate the administration of the CCTV System to another staff member.

7.4 In certain circumstances, the recordings may also be viewed by other individuals in order to achieve the objectives set out above. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

8. Access

8.1 Recorded data/images will be securely stored in a restricted place. Unauthorised access will not be permitted at any time. The area will be locked when not occupied by authorised personnel. A log of access will be maintained.

8.2 Access to the CCTV system and stored images will be restricted to authorised personnel only.

8.3 A record of the date of any disclosure request along with details of who the information has been provided to (the name of the person and the organisation they represent), why they required it and how the request was dealt with will be made and kept, in case of challenge.

8.4 Data will be provided to those requests authorised in a permanent format where possible. If this is not possible the data subject will be offered the opportunity to view the footage.

8.5 In relevant circumstances, CCTV footage may be accessed by any of the following:

- by the police where Council is required by law to make a report regarding the commission of a suspected crime;
- following a request by the police when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on or near Council property;
- by the HSE and/or any other statutory body charged with child safeguarding; or
- by data subjects (or their legal representatives), pursuant to a Subject Access Request;
- by individuals (or their legal representatives) subject to a court order; and
- by Council's insurance company where it requires same in order for Council to pursue a claim for damage done to the insured property.

9. Subject Access Requests (SAR)

9.1 Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act.

9.2 Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified, for example, date, time and location.

9.3 Council will respond to requests within 30 calendar days of receipt in accordance with the Individual Rights specified in Council's Data Protection Policy (General).

9.4 Council reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

9.5 A record of the date of the disclosure along with details of whom the information has been provided (the name of the person and where applicable the organisation they represent), and why they required it, will be made.

9.6 In giving a person a copy of their data, Council will provide a still/series of still pictures and/or an electronic form of the relevant images. However, other images of other individuals will be obscured before the data is released.

10. Complaints

Complaints about the operation of CCTV will be dealt with in accordance with Council's Complaints Policy and Procedure which is available on its website.

11. Staff Training

11.1 Staff authorised to access the CCTV system will be trained to comply with this Policy. Staff will understand that all information relating to the CCTV images must be handled securely.

11.2 Staff will receive appropriate training to enable them to identify and handle different requests according to regulations.

11.3 Staff misuse of surveillance system information will lead to disciplinary proceedings.

12. Responsibilities

12.1 The Clerk (or nominated staff member) will:

- ensure that the use of CCTV systems is implemented in accordance with this Policy;
- oversee and co-ordinate the use of CCTV monitoring for safety and security purposes;
- ensure that all existing CCTV monitoring systems are evaluated for compliance with this Policy;

- ensure that Council's CCTV monitoring is consistent with the highest standards and protections;
- review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this Policy;
- maintain a record of access (e.g. an access log) to or the release of tapes or any material recorded or stored in the system;
- ensure that the perimeter of view from fixed location cameras conforms to this Policy;
- give consideration to residents' complaints, if any, regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment;
- ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals and be mindful that no such infringement is likely to take place;
- ensure that cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "Reasonable Expectation of Privacy";
- ensure that monitoring footage are stored in a secure place with access by authorised personnel only;
- ensure that images recorded are stored for a period not longer than 30 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil);
- ensure that when a zoom facility on a camera is being used, there is a second person present with the operator of the camera to guarantee that there is no unwarranted invasion of privacy;
- ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics; and
- ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas.

Policy effective from: 21 June 2021

Date for next review: 21 June 2023 (or earlier if relevant legislation changes before this date)

In the picture: A data protection code of practice for surveillance cameras and personal information

ico.
Information Commissioner's Office

Contents

1. Introduction

The Information Commissioner's Office (ICO) issued its first code of practice under the Data Protection Act 1998 (DPA) covering the use of CCTV in 2000. The code was developed to explain the legal requirements operators of surveillance cameras were required to meet under the Act and promote best practice. The code also addressed the inconsistent standards adopted across different sectors at that time and the growing public concern caused by the increasing use of CCTV and other types of surveillance cameras.

A lot has changed since this time and, while the original code was updated in 2008, further legal, practical and technological developments mean that updated guidance is required. We have moved away from CCTV simply being a camera on top of a pole in our local town centre where the images were recorded on to video tapes, to much more sophisticated operations using digital and increasingly portable technology. The use of Automatic Number Plate Recognition (ANPR) is now commonplace and body worn cameras are being routinely used by organisations, such as the police.

Surveillance cameras are no longer a passive technology that only records and retains images, but is now a proactive one that can be used to identify people of interest and keep detailed records of people's activities, such as with ANPR cameras. The use of surveillance cameras in this way has aroused public concern due to the technology no longer being used solely to keep people and their property safe, but increasingly being used to collect evidence to inform other decisions, such as the eligibility of a child to attend a school in a particular area.

The unwarranted use of CCTV and other forms of surveillance cameras has led to a strengthening of the regulatory landscape through the passing of the Protection of Freedoms Act (POFA). The POFA has seen the introduction of a new surveillance camera code issued by the Secretary of State since June 2013 and the appointment of a Surveillance Camera Commissioner to promote the code and review its operation and impact. The ICO has contributed to this tougher regulatory landscape by taking enforcement action to restrict the unwarranted and excessive use of increasingly powerful and affordable surveillance technologies.

While the title of this code has changed to highlight its focus on the data protection implications of using CCTV and other forms of surveillance cameras, its objectives remain the same. The ICO has developed this

code following extensive consultation. It is designed to help those who use surveillance cameras to collect personal data to stay within the law.

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 individuals, and covers other information that relates to individuals, for example vehicle registration marks captured by 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 DPA and the guidance in this code will help organisations comply with these legal obligations.

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 POFA, the Human Rights Act 1998 (HRA) and the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act (POFA code).

The POFA in particular has an important role in regulating surveillance systems, creating the role of the Surveillance Camera Commissioner, which the Information Commissioner has a memorandum of understanding with to ensure effective cooperation. The Surveillance Camera Commissioner is charged with promoting good practice regarding surveillance cameras and to encourage compliance with the POFA code.

The POFA code is also an important document to refer to when your issue is not a data protection one. It provides advice and guidance on issues such as operational requirements, technical standards and the effectiveness of the systems available. The 12 guiding principles are the

key component of the POFA code and these are referenced throughout the ICO code to enable practitioners to see the core compliance points in both codes. The guiding principles in the POFA code are also contained in annex 3.

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

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

The POFA requires relevant authorities to have regard to guidance in the POFA code. In general terms, the police, police and crime commissioners and local authorities in England and Wales are designated as relevant authorities, along with the National Crime Agency. All other data controllers are encouraged to follow the POFA code and advice from the Surveillance Camera Commissioner as good practice. This code outlines the connections it has with the POFA code to help you comply with both.

Further details can be found on the Surveillance Camera Commissioner's website.

Unlike the DPA, the POFA only applies to England and Wales and therefore is not applicable to the rest of the UK. The Scottish Government has produced its CCTV Strategy for Scotland. The strategy provides a common set of principles that operators of public space CCTV systems in Scotland must follow. The principles aim to ensure that these systems are operated fairly and lawfully and are using technologies compatible with the DPA.

This code of practice covers a wider area than the POFA code. This is because the DPA is applicable to all organisations that process personal data across the whole of the UK and has the same effect across all sectors. One of the key differences is that the private sector is required to follow this code to meet its legal obligations under the DPA. 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 organisations in England and Wales to follow guidance in the POFA code.

3. What this code covers

The majority of surveillance systems are used to monitor or record the activities of individuals, or both. 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 including:

- Automatic Number Plate Recognition (ANPR);
- body worn video (BWV);
- unmanned aerial systems (UAS); and
- other systems that capture information of identifiable individuals or information relating to individuals.

This code 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 can be exempt from the DPA.

The Court of Justice of the European Union (CJEU) issued its judgment in the case of Ryneš on 11 December 2014. In this judgment, the CJEU concluded that where a fixed surveillance camera faces outwards from an individual's private domestic property and it captures images of individuals beyond the boundaries of their property, particularly where it monitors a public space, the recording cannot be considered as being for a purely personal or household purpose.

This means that cameras attached to a private individual's home may, in certain circumstances, no longer be exempt from the requirements of the DPA under section 36. Those circumstances are likely to include where the camera monitors any area beyond the interior and exterior limits of that individual's home. This would include any camera to the extent that it covered, even partially, a public space such as the pavement or street. It would also cover cameras which captured areas such as neighbours' gardens.

This decision does not mean that using such a camera is not possible but it does mean that individuals will have to ensure that its use is legitimate under the DPA. The CJEU made clear that use of cameras to protect a property in this way can meet the legitimate interest condition in the legislation. The ICO has produced a short complementary piece of guidance for the public on how to ensure the use of a surveillance camera on a private domestic property complies with the DPA.

The ICO will continue to assess the potential wider impact of the CJEU's decision on other surveillance technologies and may add further updates to this code.

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 activities relating to journalistic, artistic and literary purposes. However, this code does apply to information collected by surveillance systems that is then provided 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 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 that 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.

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

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. You should therefore 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 justification for processing personal data. 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 an 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 regularly 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. The ICO has produced a 'Conducting privacy impact assessments code of practice' that explains how to carry out a proper assessment.

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 the pressing need the surveillance system is supposed to address, and show whether or not the system will meet this need. It should be based on reliable evidence and show 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 privacy impact assessment 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 privacy impact assessment 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 POFA code (see Appendix 3 for a full list of these guiding principles) 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 appropriate privacy impact assessment in advance has contributed to many of the data protection problems that have occurred in relation to the use of surveillance systems.

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 that you 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. If you are the organisation that makes these decisions then you are the data controller and you are legally responsible for compliance with the DPA.

Wider governance issues are also addressed in Guiding Principle 4 of the POFA code.

Where more than one organisation is involved, you should both know your responsibilities and obligations. If you make joint decisions about the purposes for, and operation of, the scheme, then both of you 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 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?
- 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. This will include situations where the surveillance system is managed by a third-party on behalf of the public authority. 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 adequately trained to deal with the differing levels of sensitivity of information. In a shared service situation it should also be made clear who is in control of what information.

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 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.

Guiding Principle 5 of the POFA code emphasises the importance of clear policies and procedures and communicating these to all who need to comply with them.

You should regularly review whether the use of surveillance systems continues to be justified. It is necessary to renew your notification with the ICO annually, 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 'code of practice on Privacy notices, transparency and control', '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 effectively for its intended purpose. 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. Encryption can provide an effective means to prevent unauthorised access to images processed in a surveillance system. However, there are circumstances where it is not possible to apply encryption.

Where encryption is not appropriate, for example, if it may have an effect on the information that you are choosing to process, then other appropriate methods should be employed to ensure the safety and security of information.

If you are going to be collecting and retaining a large amount of information, for example video footage from BWV cameras, then you may wish to store the data using a cloud computing system. You will need to ensure that this system is secure and if you have contracted with a cloud provider to provide this service, you will need to ensure that the provider can ensure the security of the information. More can be found in the ICO's guidance on the use of cloud computing.

You may wish to keep a record or audit trail showing how the information must be 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 or audit trail of this process 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 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 it's required. If it can't, this may undermine the purpose for undertaking surveillance.

Guiding Principle 9 of the POFA code reinforces the importance of safeguarding information and the Surveillance Camera Commissioner is responsible under POFA for providing advice about recommended operational and technical standards.

- How practicable is it to take copies of a recording off your system when requested by a law enforcement agency? Can this be done without interrupting the operation of the system?
- Can it be provided in a suitable format without losing image quality or time and date information?
- How can you ensure that information complies with designated standards?
- 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 and any other authorised person where it is necessary for them to see it, for example to monitor congestion for health and safety purposes, 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.

If you have set up a live streaming camera available to the public so that they can, for example, assess which route to take on their journey to work based on the level of congestion, you should ensure that it is appropriately zoomed out so that individuals cannot be identified. If individuals can be identified then this will need to be justified and shown to be necessary and proportionate.

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 personnel.

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 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 in most situations. 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.

This will help you to demonstrate compliance with Guiding Principle 7 of the POFA code.

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 the other people involved.

- Are arrangements in place to restrict the disclosure of information in a manner that is consistent with the purpose for establishing the system?

- Does anyone who 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 required it?

It is important that if you have surveillance system, or if you are intending to have a surveillance system, that you have individuals who are able to use the system to access and extract information where disclosure is appropriate.

When disclosing surveillance images of individuals, particularly when responding to subject access requests, you need to consider whether the identifying features of any of the other individuals in the image need to be obscured. In most cases the privacy intrusion to third party individuals will be minimal and obscuring images will not be required. However, consideration should be given to the nature and context of the footage.

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 that 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 be provided with that information or, if they consent to it, view that information. Information must be provided promptly and within no longer than 40 calendar days of receiving a request. Providing information promptly is important, particularly where you may have a set retention period which will mean that the information will have been routinely deleted if you take the full 40 calendar days to respond. In such circumstances it is good practice to put a hold on the deletion of the information.

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 that 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; and
- 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.

You should ensure that the design of your surveillance system allows you to easily locate and extract personal data in response to subject access requests. They should also be designed to allow for the redaction of third party data where this is deemed necessary.

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

- The details you will need to find the requester's information. This might include the date, time and location where the footage was captured, or the vehicle registration mark if they're requesting information collected by ANPR cameras
- The fee you will charge for supplying the requested information (up to a maximum of £10) and how should it be paid.
- Whether you have effectively labelled information to assist with retrieval.

- How you will provide an individual with copies of the information held.

It is important to note that where a subject access request is received for surveillance footage or other information, you are required to provide the data subject with a copy of all the information caught by the request that constitutes their personal data, unless an exemption applies. This must be done by supplying them with a copy of the information in a permanent form. There are limited circumstances where this obligation does not apply.

The first is where the data subject agrees to receive their information in another way, such as by viewing the footage. The second is where the supply of a copy in a permanent form is not possible or would involve disproportionate effort. The ICO's Subject access code of practice explains the limited circumstances in which this exception may apply. If the data subject refuses an offer to view the footage or the data subject insists on a copy of the footage, then you must do whatever is proportionate to provide the data subject with this information.

It is unlikely that providing an individual with a transcript of the footage will be enough to comply with a subject access request. This is because a transcript is unlikely to fully communicate all of the information within the footage that can be considered the data subject's personal data. You should always first attempt to provide the footage to the individual, or invite the data subject to a viewing if they consent to this.

If an individual agrees to a viewing of the footage but subsequently asks for that footage, it may be necessary, or at least good practice, to provide this footage where possible. This is particularly true given that your default position should be to provide footage where requested and the data subject is entitled to make a further subject access request for the information anyway, if they choose to.

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 and 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 it is, then the information 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 a freedom of information request as the requester could potentially use the information for any purpose and the individual concerned is unlikely to expect this. This may be unfair processing in contravention of the DPA.

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

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 information 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.[2]

This is not an exhaustive guide to handling FOI requests[3].

Note: Even where footage is exempt from FOIA or 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 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 is necessary, and should be the shortest period necessary to serve your own purpose. This should not be determined simply by the storage capacity of a system.

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

[2] 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.

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

car park when there is a two 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 VRM would be the individual's personal data.

You should not keep information for longer than strictly necessary to meet your 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.

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

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 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?
- Following this advice will help you to demonstrate that you have considered Guiding Principle 6 of the POFA 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 made available across, a computer, eg an 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?

- Have your staff been made aware that they could be committing a criminal offence if they misuse surveillance system information?
- Is the process for deleting data effective and being adhered to?
- Have there been any software updates (particularly security updates) published by the equipment's manufacturer that need to be applied to the system?

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?

Such a review will also help you to demonstrate that you have considered Guiding Principle 10 of the POFA code.

Example: A CCTV system introduced to deal with persistent anti-social behaviour during the evenings may no longer be justified if this area of the town is no longer popular during this time.

6. Selecting and siting surveillance systems

The information collected by a surveillance system must be adequate for the purpose you are collecting it. The type of surveillance system you choose and the location it operates within must also achieve the purposes for which you are using it. You should ensure that the design of any surveillance systems you purchase allows you to easily locate and extract personal data in response to subject access requests. They should also be designed to allow for the redaction of third party data where this is deemed necessary.

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 you decide that a surveillance system is required then 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 identify which equipment will address the pressing need. The equipment should only collect the necessary information to meet the purpose for which it was installed.

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 amounts of 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 plants and trees in the spring and summer.

- 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 during 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, 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 that they are being recorded 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 POFA code provides clear and practical advice on how to identify the requirements of a surveillance camera system. The ICO would recommend and expect you to comply with the same standards as recommended in this principle.

7. Surveillance technologies other than CCTV systems

Surveillance systems have advanced greatly since the last version of this code was published. This section covers some of the recently developed surveillance technologies and how to approach them. While the technologies covered in this section present new issues, the recommendations throughout the rest of this code will still be relevant.

The way the information collected by these technologies can be linked or matched together means that surveillance technologies are becoming more interconnected. This presents further issues with regards to people's personal data. If you are intending to match data together from different systems, you will need to be careful that the information you are collecting is accurate and not excessive. You should also pay attention to Guiding Principle 12 of the POFA code if you are a relevant authority under the POFA.

It is possible for data collected by a range of surveillance systems to be integrated into broader 'big data' processing systems operated by organisations. This has implications in terms of profiling, what can be learnt about individuals and how decisions are made about them. The ICO published a report on the data protection implications of big data that covers this issue in further detail.

While they may not be data controllers under the DPA, the ICO also recommends that the vendors and developers of these new emerging technologies consider privacy impact assessments and a privacy by design approach when developing their systems for market. There is also a case for the system's instructions or manuals to include information highlighting the importance of addressing data protection compliance.

As data controller, you are responsible for ensuring that the design of any surveillance systems you purchase allows you to easily locate and extract personal data in response to subject access requests. They should also be designed to allow for the redaction of third party data where this is deemed necessary.

7.1 ANPR system

The capabilities of ANPR systems and their use have increased since the last revision of this code. The amount of data collected, analysed and used, the increased ease with which ANPR systems can now be linked to databases, 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.

If you are using or intend to use an ANPR system, it is important that you undertake a privacy impact assessment to justify its use and show that its introduction is proportionate and necessary. This is particularly important

given the significant amounts of information an ANPR system can collect. For example, is the system just recording vehicle registration marks? Or is it recording images of vehicles, occupants or 'patch plates' as well? If it's the latter, make sure the amount of information being collected is justifiable.

When storing the information and cross referencing it with other databases to identify individuals, you will need to ensure that these databases are kept up-to-date and accurate and are of sufficient quality to prevent mismatches. If you are sharing the personal data you process with third parties you will need to make sure that you have a data sharing agreement with them. This agreement should ensure that the appropriate safeguards are in place to keep the information secure.

You will need to ensure that you have retention periods in place for the personal data which you collect and store. The retention period should be consistent with the purpose you are collecting the data for. The information should be kept for the minimum period necessary and should be deleted once it is no longer needed.

Given the significant amounts of information that ANPR systems are able to collect, it is important that individuals are informed that their personal data is being processed. The best way to do this is through signage explaining that ANPR recording is taking place and, if possible to do so, the name of the data controller collecting the information. While it is a challenge to inform motorists that they are being monitored, there are methods you can use, such as the Town and Country Planning Act (control of advertisements) Regulations 2007, to help provide this information (see section 9.1.2 for further detail).

7.2 Body worn video (BWV)

BWV involves the use cameras that are worn by a person and are usually attached to their clothing or uniform. These devices can often record both visual and audio information. They are increasingly used across different sectors, most commonly by law enforcement agencies, but their reducing cost means that even small businesses and the public are increasingly able to purchase and use such equipment.

BWV systems are likely to be more intrusive than the more 'normal' CCTV style surveillance systems because of its mobility. Before you decide to procure and deploy such a system, it is important that you justify its use and consider whether or not it is proportionate, necessary and addresses a pressing social need. If you are going to use audio recording as well as

visual recording, the collection of audio and video needs to be justifiable. It is highly recommended that you undertake a privacy impact assessment to demonstrate that this is the case.

BWV devices have the ability to be switched on or off, but it is important to know when and when not to record. Continuous recording will require strong justification as it is likely to be excessive and cause a great deal of collateral intrusion. This is because continuous recording is likely to capture people going about their daily business, as well as the individual who is the focus of your attention. Remember that the presence of audio recording adds to the privacy intrusion (further detail on audio recording can be found in section 8 of this code). Further justification will be required if you are thinking of recording in more sensitive areas, such as private dwellings, schools, care homes etc. The pressing social need will have to be far greater in order for the use of BWV systems to be necessary and proportionate. This will require the operator to provide more evidence to support its use in this situation.

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

If you want to use a BWV system that includes both video and audio recording, the most privacy friendly approach is to a purchase a system where video and audio recording can be controlled and turned on and off independently of each other. These two types of data processing should be considered as separate data streams and consideration should therefore be given to controlling them separately to ensure that irrelevant or excessive data is not obtained and held. Organisations may feel constrained by what is available on the market in terms of independent controls for audio and video, however this does not preclude organisations specifying the features they require and getting system providers to respond to these demands. The ICO also recommends that system manufacturers consider the advice contained in this code.

Where your BWV system cannot record audio and video separately, it should only be used where the recording of audio and video together can be justified. This is important as there will be situations where either audio recording or visual recording will be more intrusive (generally audio

recording is likely to be more intrusive but visual recording may be more intrusive in particular situations, for example, where you encounter somebody in a state of undress). You should therefore assess both visual and audio recording for their privacy intrusion. It is therefore important that you identify a BWV system which has the ability to be controlled in such a manner at the procurement stage, or request a bespoke system be produced that has this ability.

Individuals using BWV systems should be able to provide sufficient fair processing to data subjects. As BWV cameras can be quite small or discreet, and could be recording in fast moving or chaotic situations, individuals may not be aware that they are being recorded. It is therefore important that clear signage is displayed, for example on an individual's uniform, to show that recording is taking place and whether the recording includes audio. You should also think of ways to provide further information to data subjects if they wish to find out more information, for example, directing them to the privacy notice on your website, if you have one.

Because of the volume of personal data and potentially sensitive personal data that BWV cameras will process and the portability of them, it is important that you have appropriately robust technical and physical security in place to protect this information. For example, make sure devices can be encrypted, or where this is not appropriate have other ways of preventing unauthorised access to information.

However, BWV cameras are part of a larger workflow of information. You will need to make appropriate decisions about retention and disposal. As you may be recording a large amount of information, you need to ensure that you can store all of it and have a retention and disposal policy in place. The policy must set out how long the information should be kept for (this should be the minimum amount of time necessary to fulfil its original purpose) and when it should be disposed of, so that you do not hold excessive amounts of personal data. You should also consider whether you need to retain all of the footage captured by a device, or whether extracting short clips would be more appropriate.

The information should be stored so that recordings relating to a specific individual or event can be easily identified, located and retrieved. You should also store the data in a way that remains under your sole control, retains the quality of the original recording and is adequate for the purpose for which it was originally collected.

You should continue to monitor the use of the BWV system as a whole to see if it is still achieving its original purpose. If it appears that it is no longer achieving this purpose or it is no longer required, you should look at potentially less privacy intrusive methods to address the need.

If you are regularly going to share recorded information with third parties then it is important that you have a data sharing agreement in place with them.[4]

7.3 Unmanned Aerial Systems (UAS)

UAS refer to the whole system under which unmanned aerial vehicles (UAV) operate. They are also referred to using different names such as Remotely Piloted Aircraft Systems (RPAS) and drones. UAV are unmanned vehicles which, if fitted with a camera, are capable of recording images whilst airborne. These devices can vary in size from the very large, up to the size of a plane, to the very small, which can be the size of a remote control plane or helicopter. They were first used by the military, but are now much more affordable and, as with BWV systems, the smaller devices can be easily purchased by businesses and members of the public.

A distinction should be drawn between those individuals who can be considered as 'hobbyists' and are therefore generally using their device for domestic purposes, and those individuals or organisations who use the device for professional or commercial purposes. Where UAS are used for non-domestic purposes, operators will need to comply with data protection obligations and it will be good practice for domestic users to be aware of the potential privacy intrusion which the use of UAS can cause to make sure they're used in a responsible manner.

Example: A business may purchase UAS 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.

The use of UAS have a high potential for collateral intrusion by recording images of individuals unnecessarily and therefore can be highly privacy intrusive, ie the likelihood of recording individuals inadvertently is high,

[4] For more advice on the use of BWV systems please see the College of Policing's guidance.

because of the height they can operate at and the unique vantage point they afford. Individuals may not always be directly identifiable from the footage captured by UAS, but can still be identified through the context they are captured in or by using the devices ability to zoom in on a specific person. As such, it is very important that you can provide a strong justification for their use. As with all of the other technologies discussed in this section, performing a robust privacy impact assessment will help you decide if using UAS is the most appropriate method to address the need that you have identified.

As with other technologies discussed, it is important that the recording system on UAS can be switched on and off when appropriate. This is particularly important given the potential for the cameras to capture large numbers of individuals from a significant height. Unless you have a strong justification for doing so, and it is necessary and proportionate, recording should not be continuous. This is something which you should look at as part of the privacy impact assessment.

UAS cover the whole system, rather than just the device in the air, so you need to ensure that the whole system is compliant. You should ensure that any data which you have collected is stored securely, for example by using encryption or another appropriate method of restricting access to the information. You should also ensure that data is retained for the minimum time necessary for its purpose and disposed of appropriately when no longer required.

You may be able to reduce the risk of collateral intrusion by incorporating privacy by design methods. For example, you may be able to procure a device that has restricted vision so that its focus is only in one place. Privacy by design can be incorporated into your privacy impact assessment and can form part of your procurement process.

One major issue with the use of UAS is the fact that on many occasions, individuals are unlikely to realise that they are being recorded, or may not know that UAV have a camera attached. The challenge of providing fair processing information is something that you must address if you decide to purchase UAS.

You will need to come up with innovative ways of providing this information. For example, this could involve wearing highly visible clothing identifying yourself as the UAS operator, placing signage in the area you are operating UAS explaining its use and having a privacy notice

on a website that you can direct people to, or some other form of privacy notice, so they can access further information.

Although these issues are the same as for any aerial vehicle with an attached camera, we have focused here on how UAS can be used as they are a novel device with the potential for a greater impact on privacy

7.4 Automated recognition technologies

The use of technologies to identify individuals' faces, the way that they walk or their eye movements, for example when they are looking at advertising, are being increasingly used by organisations. These types of technologies attract the same data protection concerns as those discussed already in this code. If you are thinking of using these systems you must provide fair processing information to data subjects. If you are storing this information you will also need to have an appropriate retention and disposal schedule and have suitable technological and physical security measures in place.

If you are using cameras to identify people's faces, you must ensure that you use high quality cameras to make sure you are capturing the individual accurately enough to fulfil the intended purpose. The results of this automatic matching should be monitored by a trained individual to ensure that there haven't been any mismatches.

Any use of these automated technologies should involve some level of human interaction and should not be done on a purely automated basis.

7.5 Privacy impact assessments and privacy by design

Clearly all of these 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 very important that you perform a privacy impact assessment. 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. Privacy impact assessments are also beneficial because consultation is a key element of

the process; this will help you to understand the public's reaction to your proposal and people's views about potential privacy intrusion.

If you are 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, you should make sure the equipment has the ability to be switched on or off, if this is appropriate, so that recording is not continuous, or be able to switch off either image or sound recording independently of each other where to capture of both would be excessive. Unless continuous recording can be shown to be justified, you should only record when it is necessary and is done for the specific purpose it is being used for. The equipment must 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 privacy impact assessment 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.

7.6 Privacy notices

It is clear that these and similar devices present more difficult challenges in relation to providing individuals with fair processing information, which is a requirement under the first principle of the DPA. For example, it will be difficult to ensure that an individual is fully informed of this information if the surveillance system is airborne, 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 unless you make all reasonable efforts to provide fair processing information. 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: In addition to more traditional methods, it may be useful to use social media to inform individuals that certain types of surveillance systems are in operation at a specific time and in a specific area. Further

links can be provided to privacy notices so that data subjects can find out more information if they are interested. This would essentially function as a layered privacy notice.

One of the main rights that a privacy notice helps deliver 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 to deal with the different issues that may arise when responding to a subject access request. If you're a public authority you will also need to consider your response to freedom of information requests.

8. Using the equipment

It is important that a surveillance system produces information that is of a suitable quality to meet the purpose for which it 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 lower 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 (for example, when the UK switches between summer and winter time)?
- 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? Guiding Principle 12 of the POFA code addresses this issue.

The Surveillance Camera Commissioner is responsible under the POFA code for providing advice on recommended operational, technical and occupational competency standards.

Surveillance systems should not normally 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 an independent sound recording facility then you should turn this off or disable it in some other way, unless you can clearly justify its use with robust supporting evidence. If you cannot control sound recording separately you will need to consider how privacy intrusive the system is as a whole, including the recording of sound.

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

The use of audio recording, particularly where it is continuous, will, in most situations, be considered more privacy intrusive than purely visual recording. Its use will therefore require much greater justification. Audio recording should only be used where:

- You have identified a need or issue which can be characterised as a pressing social need and can evidence that this need must be addressed.

1. You have considered other less privacy intrusive methods of addressing the need.
2. Having reviewed the other less privacy intrusive methods, you have concluded that these will not appropriately address the identified issue and the only way to address the issue is through the use of audio recording.
3. You should ensure that at the point of purchase of the audio system all appropriate privacy by design methods have been incorporated into the system. If you have already bought the system, you should

look to see if you can incorporate any privacy by design technologies.

4. If you are using audio recording you should make sure that the system you have bought provides a high enough quality of recording to achieve your stated aim.
5. You should make it clear to data subjects that audio recording is taking place, over and above any visual recording which is already occurring.
6. The best way to make sure these requirements are met is to carry out a thorough privacy impact assessment. (Please also see section 7.2 for specific detail on audio recording in relation to BWV systems).

Below are some examples of where audio monitoring and recording may be justified. However, if you can evidence that you have gone through the process above, you may be able to justify other uses of audio recording.

- 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 so it might be used as evidence in an investigation, 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 requiring taxis to carry out continuous video and audio recording in order to gain a license to operate in the city. The ICO and ultimately the First-Tier Tribunal (Information Rights) considered this to be a breach of principle one of the DPA, ruling that the measure was disproportionate and not justified under article 8 of the HRA (the right to private life). The argument above would similarly apply to other forms of public transport, unless clear justification for continuous recording can be provided.

Some CCTV has the ability to broadcast messages to those under surveillance. You should only use this option when the messages directly relate to the purpose for which the system was installed.

- 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 when they are in an area where a surveillance system is in operation.

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 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 in areas where people are less likely to expect that they will be monitored by a surveillance system. This is particularly important when an ANPR system is being used that covers a large area.

In exceptional circumstances where 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 a 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.

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?

Guiding Principle 3 of the POFA code promotes transparency and regular engagement with those that are likely to be monitored. This is a vital part of assessing whether any surveillance is justified and that its purpose is understood.

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

Appropriate signs must be provided to alert drivers to the use of cameras on the road network or in areas that vehicles have access to, such as car parks. It is important that these signs do not affect the safety of road users. You should consider the amount of time the driver will have to read the information you provide; particularly where the road has a high speed limit. Signs must make clear that cameras are in use and explain 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 with their data. Where authorised signs under road traffic sign regulations are used and these don't explain which organisation is operating the cameras 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.[5]

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, Northern Ireland and Scotland without an SIA licence.

- 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?

[5] See guidance on automated decision taking and the right to prevent processing.

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 the Guide to Data Protection.

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. This decision should be reviewed on a regular basis.			
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.			

[1]Not all small businesses need to notify. Current notification requirements can be found here.

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 (eg 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.

Appendix 3

The guiding principles of the Surveillance Camera Code of Practice

System operators should adopt the following 12 guiding principles:

Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.