



**SURVEILLANCE CAMERA
COMMISSIONER**

Surveillance Camera Code of Practice

A Guide for Councillors

How well does your authority comply with the 12 guiding principles of the [surveillance camera code of practice](#)?



Executive Summary

The Protection of Freedoms Act 2012 introduced legislation governing the use of surveillance camera systems that monitor public space. This included:

- The Surveillance Camera Code of Practice (2013) and The Surveillance Camera Commissioner whose role it is to encourage compliance, review operations and provide advice about the code.
- Section 33(5) places Local Authorities on a list of 'relevant authorities' who MUST pay due regard to the code.

As a Councillor you will undoubtedly want to ensure your council is compliant with the code. The requirement to comply with the code applies to all surveillance camera systems (including CCTV, Body Worn Video and Automatic Number Plate Recognition) used by your authority, and not just those monitoring streets and town centres. It includes systems in libraries, leisure centres and town halls.

The code sets out 12 principles for the operation of surveillance camera systems. Each system should:

1. Have a defined purpose and legitimate aim
2. Not impinge on an individual's privacy or human rights
3. Be operated transparently so people know they are being monitored
4. Be operated with good governance
5. Have clear policies, rules and procedures in place
6. Store no more images/data than strictly required
7. Have safeguards in place in relation to who can view images/data
8. Meet relevant and approved standards
9. Ensure images/data are stored securely
10. Review systems regularly (at least annually)
11. Be effective in supporting law enforcement
12. Databases used for matching purposes should be accurate and up to date

This guide explains what you need to know about the surveillance camera code of practice and what it means for the camera systems your authority operates.

Furthermore, we have developed an easy to use self assessment tool which can be used to assess how closely your authority is complying with the code.

Background

The Protection of Freedoms Act 2012 introduced the regulation of public space surveillance cameras in England and Wales. As a result the surveillance camera code of practice was issued by the secretary of state under Section 30 of the Act to ensure that the use of cameras in public places is regulated and only used in pursuit of a specified purpose. The code, which came into force on 12 August 2013, seeks to balance the need for cameras in public places with individuals' right to privacy.

The code applies to the use of surveillance camera systems that operate in public places in England and Wales, regardless of whether or not there is any live viewing, or recording of images or information or associated data.

All relevant authorities must have regard to the code.

A relevant authority as defined by section 33(5) of the Protection of Freedoms Act 2012 includes all local authorities in England and Wales. This includes parish and town councils. Each council therefore has to ensure that it complies with the code when it operates any surveillance camera system that monitors public space.

Local authority use of surveillance camera

Over the last twenty-five years councils have made a considerable investment in surveillance camera systems. Often this has been due to local demand for the introduction of CCTV cameras to address concerns about crime and disorder. However some have been critical of the increasing use of CCTV and the impact this has on privacy. As time and technology have progressed the ways in which surveillance cameras can be used has diversified, with some councils looking to use CCTV to address alcohol related crime and disorder and increase the safety of passengers and drivers of taxis and private hire vehicles. Others have installed systems in council facilities to reassure users, with systems monitoring libraries and leisure centres as well as being installed in council offices and town halls.

All these systems need to be operated in compliance with the code. In order to ensure it is compliant, each council needs to understand what surveillance systems it is using including public space CCTV, Automatic Number Plate Recognition (ANPR), Body Worn Videos (BWV) and Unmanned Aerial Vehicles (Drones).

To understand what your authority is using surveillance systems for; it is essential that an operational requirement is completed for each system. This will help to identify and specify the desired capabilities of the system as well as provide a basis for determining the effectiveness and suitability of the system before it is deployed. If surveillance is considered the best option, then an operational requirement will also help your authority to document the process ensuring that the proposed system is fit for purpose, has sufficient funding and public approval as well as specifying the technical requirements and a review process.

In considering whether it is compliant with the code your authority also needs to consider the circumstances in which it advocates or requires the use of surveillance cameras. It is important to note that blanket licensing policies, such as for public houses and taxis are not acceptable and there must be a pressing need and legal justification for the use of surveillance.

Issues to be addressed

Your authority needs to be aware of the number of cameras it has deployed as well as how they are deployed. It is recommended that local authorities nominate a single point of contact to oversee all the surveillance systems in the local authority and ensure that all systems are compliant with the Code.

This is vital to avoid a number of scenarios of misuse such as:

- The use of body worn cameras without appropriate training and procedures
- Use of re-deployable cameras with no operational requirement or privacy impact assessment
- Cameras with inappropriate or no signage
- The use of cameras in library, leisure centre, schools, environmental areas and waste disposal vehicles that are not compliant with the code of practice and the Data Protection Act
- No single point of contact for all local authority public space surveillance

There are a number of principles guiding the use of surveillance systems that your authority needs to consider when dealing with requests for additional cameras or systems in your area.

The Surveillance Camera Code of Practice

The code of practice is made up of 12 guiding principles and it is important that these principles are considered when using a surveillance system within a public space as defined by the code.

These principles should be considered before installing a new camera or camera system and also be applied to surveillance systems that have already been set up. To monitor compliance, if your council is yet to do so, you should ask your officers whether they have reviewed all the surveillance systems in your area. This will help you to identify what systems your authority has and why it has them.

The office of the surveillance camera commissioner has produced a simple self assessment tool that will enable your council to assess its level of compliance to the twelve guiding principles. It is important that your council identifies all surveillance systems it uses and completes the self assessment tool for each system.

Adhering to the code of practice will ensure that the use of surveillance systems in your authority is legal and being used in response to a pressing need. It will also assist in ensuring that the public space surveillance is effective, proportionate and transparent.

The self assessment tool can be found at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/372082/Self_assessment_tool_v3_WEB.pdf

The principles

Principles you need to consider regarding the surveillance systems used in your jurisdiction

Principle one

Purpose: 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.

It is important that any surveillance systems in your council have clearly defined purposes, so please check to make sure that the purposes are legitimate and have been clearly written down.

Questions your officers should consider about any system include:

- What is the system for?
- Does it have clear objectives?
- Is the system reviewed frequently against its stated purpose?
- Has it been used for anything other than its original purpose?
- If yes, what was the justification?

Principle two

Privacy: 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.

The use of any form of surveillance will have an impact on individual's privacy and rights under the Human Rights Act. As a result it is essential that this is considered in detail before a system is installed. A privacy impact assessment should be conducted in order to consider any impact the surveillance system will have on individuals and groups in the society and this impact must be proportional and justifiable. When considering plans and proposals to install new systems you should ask your officers:

- Is surveillance the best solution for the problem they are seeking to address?
- Have they conducted a privacy impact assessment?
- If yes, has it been published?
- Have they taken necessary steps to reduce any impact on individual's privacy? (such as the use of privacy zones)

Principle three

Transparency: 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.

People in a public place should be made aware that they are being monitored therefore there must be signs in place informing them that they are in a surveillance zone. The sign should have basic information including contact details for the owner of the system.

In order to ensure transparency, as much information about the system as possible should be published, this could include the number of cameras, purpose, crime statistics and consultation outcomes. In summary:

- Does your council have adequate signage?
- Has your council adequately engaged with those affected by the cameras?
- Does your authority publish information regarding the cameras on its website?
- Does your council have a procedure for handling concerns and complaints about the use of the surveillance systems?
- Are the public aware of how to make a complaint?

Principle four

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

There must be established governance arrangements for the surveillance systems in your council. If a system is jointly owned then the lines of responsibilities must be agreed and made known to all relevant parties. Questions to consider include:

- Who owns the system?
- Is the system jointly owned?
- Are there clear established lines of responsibilities
- Does the council have a designated individual responsible for the development and operation of the system?
- Are all staff aware of their responsibilities?
- Are all staff aware of the lines of responsibilities

Principle five

Rules, Policies and Procedures: 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.

The existence of clear policies and procedures are essential to meet any legal obligations regarding the use of the surveillance system such as compliance with the Data Protection Act. Once policies are in place they should be communicated to all staff and in particular to new staff at the induction stage.

You should find out whether your operators are required to have a Security Industry Authority (SIA) licence. Information on licensing requirements can be found on the SIA website at <http://www.sia.homeoffice.gov.uk/Pages/licensing.aspx>

Things to consider include:

- Does your council have clear policies in place?
- Have they been communicated to all staff and are they clearly accessible?
- Has your authority considered qualifications relevant to the role of the system users?
- Has your council considered the use of an SIA licence for its operators?

- How does your council ensure that its system users have the relevant skills and knowledge for the job?

Principle six

Storage: 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.

It is important that images and information from the surveillance camera systems are not kept for longer than is necessary to accomplish the original purpose for which they were installed. Things to consider include:

- How long are the images and information retained?
- Does your council have a policy on retention for law enforcement purposes?
- How does your council ensure that law enforcement agencies are aware of the retention policy?
- Is there an audit process to ensure that images and information are not stored for longer than necessary?

Principle seven

Access: 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.

It is essential to ensure that there is limited and restricted access to the stored information. As a result there should be clear rules on to whom and when access is allowed. An operator must have clear policies and guidelines to deal with any requests to view information.

As individuals are entitled to a copy of images of themselves, it is essential to have a policy on place to deal with subject access requests.

Things to ask should include:

- Does your council have a policy in place on who has access to the stored information?
- What is your council's policy on disclosure of information? Are all staff aware of these policies
- What checks are in place to ensure that these policies and procedures are followed?

Principle eight

Approved Standards: 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.

It is important to consider any approved standards for the installed system. This could be for the functioning, installation, operation and maintenance of the system. This is particularly important when there is a specific deployment requirement such as the use of body worn cameras.

A list of approved standards is available on the Surveillance Camera Commissioner's website at <https://www.gov.uk/recommended-standards-for-the-cctv-industry>

Things to consider include:

- What approved operational, technical and competency standards relevant to a surveillance system and its purpose does your council's system(s) meet?
- How does your council ensure that these standards are followed appropriately?
- What steps are in place to secure certification against the approved standards?
- Have your officers considered certification against the surveillance camera code of practice?

Principle nine

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

It is essential to have effective safeguards to help ensure the integrity of the images and information particular if they are necessary as evidence in court proceedings. It is important to ask the following:

- What security safeguards does your council have in place to ensure the integrity of images and information?
- If the system is connected across an organisational network or intranet, do sufficient controls and safeguards exist?
- What is the specified purpose for which the information are being used and accessed and is this consistent with the stated purposes?
- Does your council have preventative measures in place to guard against misuse of information and images?
- Are your council's procedures and instructions and/or guidelines regarding the storage, use and access of surveillance system information documented?

Principle ten

Review and Audits: 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.

It is good practice to review the continued use of a surveillance camera system on a regular basis, at least annually, to ensure that it remains necessary, proportionate and effective in meeting its specified purpose.

- How frequently is the system reviewed? (recommended to be at least annually)
- Does your council have a review process that shows its system(s) still addresses the needs and delivers the benefits that justify its use?
- Has your council identified any cameras that do not remain justified in meeting the stated purpose(s)?
- Have your officers conducted an evaluation in order to compare alternative interventions to surveillance cameras?
- Is it cost effective to continue running your council's surveillance camera system?

Principle eleven

Support Law Enforcement: 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.

The effectiveness of your council's system is dependent on its ability to capture, process, analyse and store images and information. This is particularly important if the purpose of your authority's system includes the prevention, detection and investigation of crime. If this is the case your council's system should be capable of producing images and information that are suitable for the criminal judicial system. Things to consider include:

- Are the images and information produced by your authority's system of a suitable quality for the criminal justice system to use without enhancement?
- During the production of the operational requirement for your council's system, what stakeholder engagement was carried out or guidance followed to ensure exported data would meet the quality required for it to be used for evidential purposes?
- Does your council have safeguards in place to ensure the forensic integrity of the images and information including a complete audit trail?
- Does your council have a policy on data storage, security and deletion?
- Is the information stored in a format that is easily exportable?
- Does the storage ensure the integrity and quality of original recording and the meta data?

Principle twelve

Reference Database: 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.

If your council uses specific technologies such as ANPR or facial recognition, you should satisfy yourself that the underlying data is accurate and fit for purpose. It is important to consider the following questions:

- Does your council use any specialist technology such as ANPR, facial recognition, Body Worn Video (BWV) or remotely operated vehicles (Drones)?
- Does your council have a policy in place to ensure that the information contained on its database is accurate and up to date?
- Does your council have a procedure for deciding when and whether an individual or vehicle should be included in a reference database?
- What policies are in place to determine how long information remains in the reference database?
- Are all staff aware of when surveillance becomes covert surveillance under the Regulation of Investigatory Powers Act (RIPA) 2000?