



OFFICE OF THE BIOMETRICS
AND SURVEILLANCE
CAMERA COMMISSIONER

Surveillance Camera Code of Practice

A Guide for Local Authorities

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 governs the use of surveillance camera systems¹ that monitor public spaces. This includes:

- The [Surveillance Camera Code of Practice](#) (revised in 2021) and the Biometrics and 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 Local Authority you will undoubtedly want to ensure your authority is compliant with the Code. The requirement to comply with the Code applies to all surveillance camera systems/VSS, (including CCTV, Body Worn Video (BWV), Automatic Number Plate Recognition (ANPR), Unmanned Aerial Vehicles (UAV or drones) and vehicle-borne video systems) used by your authority, and not just those monitoring streets and town centres. This includes, but is not limited to surveillance camera systems/VSS installed at libraries, leisure centres, town halls, schools, museums, housing estates and communal residential areas, parks and open spaces, cemeteries, waste and recycling facilities, transport hubs and any other local authority owned or managed sites where surveillance cameras are deployed for public safety, security and community protection purposes,

The Code sets out 12 principles for the operation of surveillance camera systems/VSS. 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 or information than strictly required
7. Have safeguards in place in relation to who can view images or information
8. Meet relevant and approved standards
9. Ensure images or information 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

¹ The term “*Surveillance Camera Systems*”, as used in the Protection of Freedoms Act 2012 (PoFA), is increasingly being replaced in contemporary usage by “*Video Surveillance Systems (VSS)*”. For the purposes of consistency and clarity, both terms have been used in this document, and they refer to surveillance systems such as public space CCTV, Automatic Number Plate Recognition (ANPR), use of Facial Recognition Technologies (FRT), Body Worn Videos (BWV), Unmanned Aerial Vehicles (UAV or Drones) and vehicle borne video systems, which would constitute local authority owned vehicles, such as parking enforcement cars, rubbish and waste collecting lorries and/or any other authority owned or managed vehicles with dash cams, rear-view or side mounted cameras.

This guide explains what you need to know about the Surveillance Camera Code of Practice and what it means for the surveillance camera systems/VSS 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 was first introduced in August 2013 and was subsequently updated, with the revised Code taking effect on 12 January 2022. It 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/VSS 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 and, if they decide to depart from it, must have and give clear reasons for doing so.

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 authority therefore has to ensure that it complies with the Code when it operates any surveillance camera system/VSS that monitors public space.

Local authority use of surveillance cameras

Over the last twenty-five years local authorities have historically made considerable investment in surveillance camera systems/VSS. Often this has been due to local demand for the introduction of VSS to address concerns about crime, disorder and public safety. However, some have been critical of the increasing use of VSS and the impact this has on privacy. As time and technology have progressed the ways in which surveillance cameras can be used have diversified. Some local authorities now deploy VSS to address alcohol-related crime and disorder and to improve the safety of passengers and drivers of taxis and private hire vehicles. Surveillance cameras have also become standard equipment on many forms of local authority-owned and managed public service and commercial vehicles, including buses, trains, refuse collection and enforcement vehicles. In addition, many authorities have installed surveillance systems/VSS within their facilities to reassure users, with systems in place at libraries and leisure centres as well as being installed in civic offices and town halls.

All these systems need to be operated in compliance with the Code. In order to ensure it is compliant, each local authority needs to understand what surveillance systems/VSS it is using including public space CCTV, Automatic Number Plate Recognition (ANPR), Body Worn Videos (BWV), Unmanned Aerial Vehicles (UAV or Drones) and vehicle borne video systems.

Local authorities must be able to demonstrate compliance with the principles of the Code for all surveillance systems/VSS they operate. If an authority is unable to meet or maintain these requirements, it should not deploy or continue using those systems.

To understand what your authority is using surveillance systems/VSS 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 systems/VSS. 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/VSS in the 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 or the 'switching on' or enabling of recognition technologies on existing surveillance systems/VSS with no operational requirement or data protection impact assessment.
- The use of cameras with inappropriate or no signage.
- The use of cameras that are not compliant with the Code of Practice, the Data Protection Act (2018) or UK GDPR (2021).
- No single point of contact for all local authority public space surveillance.
- Use of reference databases, for recognition technologies, that are inaccurate or not subject to regular validation.

- The covert use of video surveillance systems, governed by the Regulation of Investigatory Powers Act 2000 and overseen by the Investigatory Powers Commissioner.

There are a number of principles guiding the use of surveillance systems/VSS that your authority needs to consider when dealing with requests for additional cameras or systems in your area. These are enshrined in the Surveillance Camera Code of Practice.

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/VSS within a public space as defined by the Code.

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

The Office of the Biometrics and Surveillance Camera Commissioner has produced a simple self-assessment tool that will enable your authority to assess its level of compliance to the twelve guiding principles. It is important that your authority identifies all surveillance systems/VSS 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/VSS 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:

[Surveillance camera code of practice: self-assessment tool](#)

The principles

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

Principle one

Purpose: Use of a surveillance camera system/VSS 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/VSS in your authority 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 documented in writing?
- Is the system necessary or are there other ways of achieving the same purpose?
- 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 for surveillance being a necessary and proportionate response?

Principle two

Privacy: The use of a surveillance camera system/VSS 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 and may engage obligations under the Data Protection Act (2018), the UK GDPR (2021), the Data Use and Access Act (2025), the Human Rights Act (1998), and the Equality Act (2010). As a result, it is essential that these impacts are assessed in detail before a surveillance camera system/VSS is installed.

A data protection impact assessment² (DPIA) should be conducted in order to consider any impact the surveillance system/VSS 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 data protection impact assessment?
- If yes, has it been published?
- Is your camera system registered with the ICO?
- Have they taken necessary steps to reduce any impact on individual's privacy? (such as the use of privacy zones)

² The Information Commissioners Office (ICO) and OBSCC have jointly developed a Data Protection Impact Assessment (DPIA) template to support relevant authorities in assessing the privacy implications of surveillance systems/VSS. The template and accompanying user guidance can be found here: [Data protection impact assessments for surveillance cameras](#)

Principle three

Transparency: There must be as much transparency in the use of a surveillance camera system/VSS 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 signs 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 authority have adequate signage that clearly indicates surveillance is taking place, identifies the system operator, provides a contact point for enquiries, and explains how camera locations can be identified and reported?
- Do you have additional signage when Facial Recognition Technology (FRT) is deployed or activated?
- Has your authority adequately engaged with those affected by the cameras?
- Is the use of your surveillance camera system covered in your authority's Privacy Notice?
- Does your authority publish information regarding the cameras on its website?
- Are the public aware of how to make a complaint?
- Does your local authority have a procedure for handling concerns and complaints about the use of the surveillance systems/VSS?

Principle four

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

There must be established governance arrangements for the surveillance systems/VSS in your authority. 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?
- What governance arrangements are in place to ensure accountability for the surveillance camera systems/VSS, such as documenting through operational logs and records. Are there clear established lines of responsibilities?
- Does the local authority have a designated individual responsible for the development and operation of the system?

- Are all staff aware of their responsibilities and the lines of responsibility?
- Have staff been trained to use specialist technologies, do they understand how these work?

Principle five

Rules, Policies and Procedures: Clear rules, policies and procedures must be in place before a surveillance camera system/VSS 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/VSS such as compliance with the Data Protection Act (2018), the UK GDPR (2021), the Data Use and Access Act (2025), the Human Rights Act (1998), and the Equality Act (2010). 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: [Apply for an SIA licence](#).

Things to consider include:

- Does your local authority have clear documented policies and procedures (such as an internal Code of Practice) in place for the deployment and use of each type of surveillance system/VSS (such as CCTV, ANPR, BWV, UAV/drones and vehicle borne video systems)?
- Have they been communicated to all staff and are they clearly accessible?
- Do you have documented procedures for handling errors or mistakes?
- Has your authority considered qualifications or occupational standards relevant to the role of the system users?
- Has your authority considered the use of an SIA licence for its operators?
- How does your authority ensure that its system users have the relevant skills and knowledge for the job?
- If your authority deploys drones, do you have the relevant permissions from the Civil Aviation Authority (CAA)?

Principle six

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

It is important that images or information from the surveillance camera systems/VSS 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 or information retained?
- Does your authority have a policy on retention for law enforcement purposes?

- How does your authority ensure that law enforcement agencies are aware of the retention policy?
- Is there an audit process to ensure that images or information are not stored for longer than necessary?
- Is there a clear policy for the destruction of images or information?
- Do you have a process of logging and recording these deletions?

Principle seven

Access: Access to retained images or 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 or 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 and must maintain an accurate and auditable record of all data shared, including details of what was shared, with whom, when, and the lawful basis for disclosure.

As individuals are entitled to a copy of images or information of themselves, local authorities should not operate a surveillance camera system/VSS unless they are able to meet their legal obligations. This includes responding appropriately to Subject Access Requests (SARs) and facilitating individuals' rights to erasure where applicable. Local authorities must have appropriate policies and procedures in place to handle such requests and to provide information within the required timescales

Things to ask should include:

- Does your local authority have a policy in place on who has access to the stored information?
- What is your local authority's policy on disclosure of information to third parties (including the public, law enforcement or prosecuting bodies)?
- Does your local authority keep a record of who, including third parties, has been granted access to stored information and when that access was provided?
- Are all staff aware of these policies?
- What procedures do you have in place to guard against cyber risks?
- What are your procedures for handling a SAR?
- Is there information on your website informing the public on how to make a SAR or to request erasure of personal data?
- Does your local authority have methods and procedures in place to redact third-party personal data when responding to SARs?
- What checks are in place to ensure that these policies and procedures are followed?

Principle eight

Approved Standards: Surveillance camera system/VSS 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 procurement, 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 BSCC's website: [Recommended standards for the surveillance camera industry](#)

Things to consider include:

- What approved operational, technical and competency standards relevant to a surveillance system/VSS and its purpose does your local authority's system(s) meet?
- How does your authority ensure that these standards are followed appropriately?
- What steps are in place to secure certification against the approved standards?
- Have your officers considered independent accreditation against the Surveillance Camera Code of Practice?

Principle nine

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

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

- Who authorises the sharing or disclosure of images or information?
- What security safeguards does your authority have in place to protect images or information from unauthorised access/disclosure, misuse, loss, alteration and/or any other forms of compromise?
- If the system is connected across an organisational network or intranet, do sufficient controls and safeguards exist?
- How do your security systems guard against cyber security threats?
- Are your authority's procedures and instructions and/or guidelines regarding the storage, use and access of surveillance system/VSS 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/VSS on a regular basis, at least annually, to ensure that it remains necessary, proportionate and effective in meeting its specified purpose.

- Does your authority have a review process that demonstrates its system(s) still address the needs and delivers the benefits that justify its use?
- Does the review include an assessment of the need for every single camera in a system?
- How frequently is the system reviewed? (recommended to be at least annually)
- Is there a designated person responsible for conducting the review?
- Are records kept of the outcomes of review and whether any resulting actions have been implemented, including decisions that no action is required?
- How are the findings of the review reported and to whom?
- Are records kept of when the reviews were conducted and who carried them out?
- Has your authority identified any cameras that do not remain justified in meeting the stated purpose(s)? If yes, Is there an action plan for their decommissioning?
- Have your officers conducted an evaluation in order to compare alternative interventions to surveillance cameras?
- Is it cost effective to continue running your local authority's surveillance camera system/VSS?

Principle eleven

Support Law Enforcement: When the use of a surveillance camera system/VSS 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 or information of evidential value.

The effectiveness of your authority's system(s) is dependent on its ability to capture, process, analyse and store images or 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 authority's system should be capable of producing images or information that are suitable for the criminal judicial system. This requires a higher specification for images and a demonstrable integrity of systems and images. Things to consider include:

- Are the images or information produced by your authority's system of a suitable quality for law enforcement and/or the criminal justice system to use without enhancement?
- Is there a documented and clearly defined process by which law enforcement agencies can request images from your authority's system?

- What engagement or consultation was undertaken with law enforcement agencies during the development of your authority's operational requirement to ensure that exported data would be of sufficient quality and integrity for evidential use in investigations and legal proceedings?
- How do you verify that the footage or information produced by your authority's system is of a suitable quality to be used as evidence in investigations, legal proceedings, or prosecutions?
- Have any concerns or challenges been identified regarding the quality of images, footage or information provided by your authority's systems for evidential purposes in the last 12 months?
- Do you monitor or record these instances? Has the local authority adopted and used the [Framework Service Level Agreement](#) (or an equivalent arrangement) to support effective operation with third parties?
- Does your local authority have safeguards in place to ensure the forensic integrity of the images or information including a complete audit trail?
- Does your local authority have a policy on data storage, security and deletion?
- Are the images or information stored in a format that is easily exportable?
- Does the storage ensure the integrity and quality of original recording and the metadata?

Principle twelve

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

If your authority uses specific recognition 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 authority use any specialist technology such as ANPR or facial recognition, that uses functionality to compare images or information against a reference database for matching purposes?
- Does your authority have a policy in place to ensure that the information contained on its database is accurate and up to date?
- Does your authority 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?
- Do you have a process for correcting inaccurate or outdated entries on the reference database?
- Are all staff aware of when surveillance becomes covert surveillance under the Regulation of Investigatory Powers Act (RIPA) 2000?