**Contents**

[1. Introduction 3](#_Toc207789664)

[2. Definitions 3](#_Toc207789665)

[3. Purpose 4](#_Toc207789666)

[4. Scope 5](#_Toc207789667)

[5. Principles of Use 5](#_Toc207789668)

[6. Justification for use of CCTV 6](#_Toc207789669)

[7. Covert surveillance 6](#_Toc207789670)

[8. Governance of CCTV 7](#_Toc207789671)

[9. Data Protection Impact Assessment 8](#_Toc207789672)

[10. Control of CCTV System 8](#_Toc207789673)

[11. Location of cameras 8](#_Toc207789674)

[12. Transparency - Notification, Signage and Awareness 9](#_Toc207789675)

[13. Data gathering and retention 10](#_Toc207789676)

[14. Access to data 10](#_Toc207789677)

[15. Responsibilities 11](#_Toc207789678)

[Councilors and employees 11](#_Toc207789679)

[Contractors 11](#_Toc207789680)

[16. Implementation and Review 11](#_Toc207789681)

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Summary of changes** | **Author** |
| V1.0 | June 2019 | Initial | One West |
| V1.1 | Dec 2022 | Refresh | One West |
| V2.0 | Aug 2023 | School and Town Council CCTV policies consolidated | One West |
| V2.1 | Oct 2023 | Formatting changes | One West |
| V3.0 | Sep 2025 | School and Town Council CCTV policies separated | One West |

**\*\*\*Using this Template\*\*\***

**Guidance**

This template is for council to complete a policy covering the operation of their CCTV system. Writing a CCTV policy and publishing it on the council’s Internet pages will support the principles of openness and transparency.

CCTV is often used as generic term that may include use of related technology, such as ANPR or BWV as well as what is usually considered as CCTV.

Crucially, you should have or are about to complete a Data Protection Impact Assessment (DPIA) for your CCTV. The outcome of that DPIA may inform your CCTV policy. Importantly a DPIA CCTV should be completed when:

* CCTV is being considered.
* New technology or functionality is being added on to an existing system.
* There are plans to process more sensitive data
* Images will be captured from a different location

You may have to consult your IT Department or CCTV provider, as well as your DPO, while completing a DPIA.

Your use of CCTV should be considered annually to determine whether it still achieves the needs initially set out when you installed it.

**Instructions**

Please read the guidance before attempting to complete this policy.

Where you see text surrounded by square brackets ‘[ ]’ these are questions/points that you need to consider before making any changes to the document.

* Importantly, answer all questions.
* If you are unsure of the questions being asked contact One West for advice.
* Once all changes have been made, delete the square brackets and their contents.

When all points have been considered you should present the policy to the Data Controller and/or councillors for authorisation.

Where you see highlighted text replace it with the appropriate/preferred name and details.

Do not forget to update the ‘Table of Contents’ and detail the version of your policy.

Finally, *delete* this text box and save the file.

# Introduction

Since its introduction to retailers in 1967, and to town centres in 1985, the use of Closed-Circuit Television (CCTV) across the UK has become increasingly popular. CCTV, along with related forms of surveillance equipment, such as Automatic Number Plate Recognition (ANPR) and Body Worn Video (BWV), are one of the most powerful tools developed during recent years to assist with efforts to combat crime and disorder, whilst enhancing community safety.

CCTV may be regarded by some as an infringement of peoples’ liberty. [Organisation name] is committed to the belief that everyone has the right to respect for their private and family life and their home. This policy in conjunction with related processes and procedures, is intended to safeguard the integrity of [Organisation name]’s CCTV and surveillance technologies, while ensuring the right to privacy is not breached.

This policy is published on behalf of the councillors of Organisation name. This policy covers the use and management of video equipment and related technologies, such as ANPR and BWV, that is often known by the generic title ‘CCTV’ and data (images and audio) captured using them to ensure that Organisation name complies with the Data Protection Legislation and other relevant legislation. Crucially personal data is processed in line with Organisation name’s Data Protection Policy [if this is published on an Internet facing website it is suggested you create a hypertext link to your council’s Data Protection Policy]. Organisation name’s use of CCTV is cognisant of the Guiding Principles of the Surveillance Camera Code of Practice updated and published by the Home Office in 2021.

The Organisation name uses CCTV for the purposes of the prevention and detection of crime, keeping [Residents, businesses and their staff, visitors and council employees] safe and to recognise and to identify individuals with a view to taking appropriate action where necessary.

This policy and related procedures apply to all sites managed by Organisation name and wherever Organisation name has deployed its surveillance equipment.

# Definitions

**ANPR** –Automatic Number Plate Recognition(ANPR) is a technology that uses optical character recognition on images to read vehicle registration plates to create vehicle location data. It can use existing CCTV, road-rule enforcement cameras, such as speed cameras, or cameras specifically designed for the task. Vehicle location data may be used for various purposes, such as the criminal investigations, car park management and traffic management.

**BWV** - Body Worn Video (BWV) involves the use of cameras that are worn by a person and are often attached onto the front of clothing or a uniform. These devices may be capable of recording both images and audio.

**CCTV** – Closed-circuit television (CCTV) is a video surveillance system in which signals are transmitted to a specific set of monitors and are not publicly broadcast. It is primarily used for security and monitoring purposes.

**Data Controller** - a person/organisation who (either alone or with others) controls the contents and use of personal data.

**Data Processing** - performing any operation or set of operations on data, including:

* Obtaining, recording, or keeping the data,
* Collecting, organising, storing, altering, or adapting the data,
* Retrieving, consulting, or using the data,
* Disclosing the data by transmitting, disseminating, or otherwise making it available,
* Aligning, combining, blocking, erasing, or destroying the data.

**Data Processor** – a person/organisation who processes personal data on behalf of a data controller. Employees of a controller are not processors if they are acting within the scope of their duties as an employee.

**Data Protection Legislation** – this means the Data Protection Act 2018 (DPA 2018), UK General Data Protection Regulations (UK GDPR) and the Data (Use and Access) Act (in force from 19 June 2025).

**Data Subject** – a living individual who can be identified, directly or indirectly, from the personal data that is held about them.

**Directed Surveillance** – is covert surveillance in places other than residential premises or private vehicles.

**Personal Data** – is data that relates to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

**Subject Access Request** - is where a person makes a request to the organisation for the disclosure of their personal data under data protection law.

# Purpose

The purpose of this policy is to regulate the use of CCTV and associated technologies to monitor activity in council buildings and to provide public space surveillance in the town centre, public spaces, and housing estates.

This policy has been used as the basis for siting CCTV cameras and associated equipment and defines the governance surrounding the use of CCTV equipment and the related processing activities. The policy ensures that ***Data Protection by Design*** is a key consideration in all Organisation name’s CCTV processes and help ensure that the rights of data subjects are always met.

CCTV at Organisation name is intended for the purposes of:

* Protecting buildings and assets, both during and after working hours.
* Promoting the health and safety of [Residents, businesses and their staff, visitors and council employees].
* Reducing the incidence of crime and anti-social behaviour (including theft and vandalism).
* Supporting the police in a bid to deter and detect crime.
* Assisting in the identification, apprehension, and prosecution of offenders.

[**Note** Remove/add any purposes as you see fit. If the organisation plans to use CCTV to monitor staff for time management, then the Council will need to consult with staff and possibly any representatives beforehand.]

To support the principles of openness and transparency this policy will be published on the Organisation name website. The existence of this policy, and any subsequent changes to the policy, will be notified to employees and volunteers.

# Scope

This policy applies to the use of CCTV and related technologies regardless of whether there is any live viewing or recording of images or associated data/information. Covert surveillance using CCTV is not covered by this policy.

# Principles of Use

The use of a CCTV system by Organisation name follows the [12 Guiding Principles of the Surveillance Camera Code of Practice](https://assets.publishing.service.gov.uk/media/619b7b50e90e07044a559c9b/Surveillance_Camera_CoP_Accessible_PDF.pdf) that was updated and published by the Home Office in 2021. These principles are summarised below:

**Principle 1** - Use of a surveillance camera system must always be for a specified purpose that is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

**Principle 2** - The use of a surveillance camera system must consider its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

**Principle 3** - 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.

**Principle 4** - There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

**Principle 5** - 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.

**Principle 6** - 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.

**Principle 7** - 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.

**Principle 8** - 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.

**Principle 9** - Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

**Principle 10** - 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.

**Principle 11** - 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.

**Principle 12** - 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.

# Justification for use of CCTV

Organisation name has responsibility for the protection of its property and equipment as well providing security to its residents, businesses and their staff, visitors and council employees. Moreover, Organisation name owes a duty of care under the Health and Safety at Work etc. Act 1974 and associated legislation. Hence Organisation name uses CCTV and associated technologies plus monitoring and recording equipment as an additional mode of security and surveillance for each of these purposes. CCTV systems are installed (both internally and externally) on Organisation name buildings, such as libraries, leisure centres and the town hall and will operate constantly. [BWV may be worn by council employees / volunteers while conducting business on behalf of the council in those areas that are under the control of the council and while they visit other areas, such as residential areas and business areas].

Use of CCTV for security purposes will be conducted in a manner consistent with related legislation and all existing policies adopted by the council, including its Equality & Diversity Policy, Dignity at Work Policy, and codes of practice for dealing with any complaints of bullying & harassment and sexual harassment.

[Importantly CCTV will not be used to monitor normal staff activity on site].

Data Protection Laws requires that personal data is ‘adequate, relevant and not excessive’ for the purpose for which it is collected. This means that an organisation needs to be able to justify obtaining and the use of personal data by means of a CCTV system. The use of CCTV to monitor and help control its buildings etc. for security purposes has been justified by the [Council / Full Council / Facilities Committee]. The system/s are intended to capture images of intruders or of individuals damaging property or removing goods without authorisation.

In other areas where CCTV has been installed by the council, it has demonstrated before installation of the system that there is a proven risk to security and/or health & safety of residents, visitors and employees. Importantly, the coverage of the CCTV is only enough to address issues that have arisen prior to the installation of the system.

All CCTV systems and associated equipment will be required to be compliant with this policy following its adoption. Recognisable images captured by CCTV systems are ‘[personal data](http://www.dataprotection.ie/viewdoc.asp?m=m&fn=/documents/guidance/310604.htm)’. Hence, they are covered by the provisions of the Data Protection Act 2018. It is likely that information obtained in ways that violate this policy may not be used in any legal or disciplinary proceedings.

# Covert surveillance

Importantly Organisation name will not engage in covert surveillance using CCTV. Very occasionally the police may request to carry out covert surveillance using the council’s equipment. Covert surveillance will require the consent of an Authorising Officer, which may be a magistrate. Any such request made by the police will be in writing and the Organisation name may seek legal advice.

# Governance of CCTV

[Consider the description below and then select what reflects your council’s position most closely. You may have to modify the descriptions to accurately represent your council’s situation. Delete what is not appropriate.]

[The council is in direct control of its CCTV system and associated technologies. The roles and responsibilities of its staff/contractors are clearly defined. And all staff are trained to the appropriate level before using / interacting with the system. The council ensures that our CCTV system and technologies comply with all regulations. Councillors with oversight of the operation and periodic review of the performance of the council’s CCTV system and associated technologies follow the guidance in the SCC’s [Surveillance camera code of practice: guidance for councillors](https://www.gov.uk/government/publications/surveillance-camera-code-of-practice-guidance-for-councillors) that was published in 2016.]

[The council operates a public CCTV system jointly with the [Police, other local authorities or have access to third party CCTV systems]. [This approach is part of a local crime reduction strategy].

All parties work together to ensure that all elements of this joint CCTV system comply with all regulations. The governance arrangements for this joint system are clearly defined and all responsibilities were agreed before the system was commissioned. All staff are trained to the appropriate level before using / interacting with the system.

Those councillors in [organisation name] with oversight of the operation and periodic review of the performance of this joint CCTV system and associated technologies follow the guidance in the SCC’s [Surveillance camera code of practice: guidance for councillors](https://www.gov.uk/government/publications/surveillance-camera-code-of-practice-guidance-for-councillors) that was published in 2016].

The council will review the effectiveness of the CCTV system and associated technologies and confirm the arrangements surrounding the use of the system are correct on an annual basis. The council will also ensure that a risk assessment of the use of the system, DPIA, is completed annually.

Wherever there is need to share data captured by CCTV and the associated technologies there will be a Data Sharing Agreement (DSA) or a Memorandum of Understanding (MoU). These documents should define:

* Data ownership, such as ‘solely by the council’, ‘jointly with the police or other public body’ or as two separate data controllers for their own specific purposes.
* Descriptions of CCTV hubs, viewing stations or access to CCTV infrastructure.
* Data subject rights, such as access, especially where information may be requested as part of a legal case or insurance claim.
* Signage (form and positioning) and transparency information and who should produce it or maintain it.
* Training standards for operators.
* The period of retention of data and whether data is automatically overwritten.
* Additional agreements that either party may be subject to, such as the police Back Office Function 2 (BOF2) for ANPR.
* Processes that consider aspects of a CCTV system, such as camera relocation, use of facial recognition technologies or decommissioning the system.

[This is not an exhaustive list, and any agreement should be flexible enough and reviewed at an appropriate frequency to enable updates and open dialogue between parties.]

# Data Protection Impact Assessment

Prior to the adoption of any new CCTV system or where an existing system has not been assessed, legislation requires a comprehensive review of risk to personal data. This is done in the form of a DPIA. Following the DPIA process will lead to a review of the purpose or purposes for the use of CCTV, establish any impact it may have upon individuals and any risks that may be involved with the system.

The [Town Clerk or a delegated individual], will be responsible for completing the DPIA in collaboration with the council’s DPO. Should a third-party be used to operate the CCTV, the person from the [Name of council body responsible for oversight of CCTV operation] who has been delegated responsibility for its implementation will work with the contractor and the DPO to ensure that the DPIA is completed and any risks associated with operating the CCTV system/s are understood.

# Control of CCTV System

Our CCTV team operates a 24/7 CCTV control centre, continuously monitoring cameras and staying in contact with the police and other private / public bodies, such as businesses. Organisation name works year-round to support the council and external enforcement agencies, including the police. The CCTV control centre collaborates with local businesses and security personnel to help manage crime in the area. The CCTV Control Centre is operated in accordance with the law and security industry best practice

# Location of cameras

Organisation name has endeavoured to select locations for the installation of CCTV cameras to achieve the aim/s of installing CCTV while having a minimum impact on the privacy of individuals. Cameras installed to record public spaces are positioned so that they do not record images of private property.

The following locations may be covered by CCTV:

* + - * A building’s perimeter, entrances and exits, lobbies and corridors, special storage areas, and receiving areas for goods and services.
* Restricted access areas at entrances to premises and buildings and other areas. Purpose – control of access.
* Intrusion alarms, exit door controls and areas covered by external alarm. Purpose - verification of alarms.
* Parking areas, main entrance/exit gates and public places. Purpose - traffic control.
* Public spaces, shopping precincts, leisure centres, libraries, and residential areas.Purpose *-*criminal investigations (carried out by the police) robbery, theft and burglary, and detecting anti-social behaviour.

[The locations of the council’s CCTV cameras are shown at the following webpage – Organisation name – CCTV camera locations.]

[If you have the facility to create a map that shows the location of CCTV cameras you may consider publishing it on your council’s website and providing a hypertext link to that webpage in this policy].

# Transparency - Notification, Signage and Awareness

CCTV signage is necessary for transparency. Hence, to indicate that CCTV is in operation, the Organisation name displays adequate signage in buildings and in public spaces where a CCTV camera(s) is sited and used.

The signage shall include the name and contact details of the data controller, as well as details why CCTV is used.

An example of the signage used by Organisation name is shown below.

**WARNING**



**CCTV cameras in operation**

**Images are being monitored and recorded for the purpose of crime-prevention, the prevention of anti-social behaviour, for the safety of our resident, visitors and staff/employees and for the protection of** ORGANISATION NAME **and its property.**

**This system will be in operation 24 hours a day, every day.**

**These images may be passed to the police.**

**This scheme is controlled by** ORGANISATION NAME **and operated by** INSERT NAME OF COMMERCIAL SECURITY COMPANY WHERE ONE IS USED

**For more information contact** *………<phone number>…………*

Signage is places at the following locations:

* [At entrances to premises i.e. external doors, school gates.]
* [Reception area.]
* [At or close to each internal camera.]
* [At or close to each camera around the town.]

# Data gathering and retention

The Organisation name’s CCTV comprises several CCTV cameras connected to a Network Video Recorder (NVR). Imagery / video footage is stored on the NVR and can be viewed either in real-time (live) or after an event via a console. [The system is / is not normally monitored]. Where an incident occurs video footage may be referred to as part of an investigation.

A log of access will be maintained that will show who accessed the system at what time and for what purpose. Access to the console and the recorded data will be restricted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of the [Name of individual responsible. Usually the Data Controller]. They have delegated the day-to-day administration of the CCTV system to Organisation name business manager.

The CCTV imagery is held in digital format that makes it easy to transmit to other organisations. The Organisation name CCTV system is connected to / isolated from any other system. Where an external organisation, such as the police, seeks access to the council’s imagery / video footage from the CCTV, access will only be granted when a suitable application has been received by the council.

Importantly, data processed by the Organisation name CCTV ‘shall not be kept for longer than is necessary for’ the purposes for which it was obtained. The Organisation name’s CCTV system should not retain footage beyond one month (28 days). Where the images identify an issue, such as a break-in or theft etc., the images / video footage that relate to that event may be retained specifically for the purpose of an investigation/prosecution related to that issue.

# Access to data

Unauthorised access to live feeds, equipment used to store images and any additional equipment that is used to operate the Organisation name CCTV system is prohibited. A log of access to the CCTV system and its components and images / video footage is to be maintained.

Access to the CCTV system and video footage may be granted by Organisation name for the following reasons:

* + Where Organisation name (or its agents) 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 Organisation name property.
	+ To provide a report to the Health and Safety Executive and/or any other statutory body with the powers of investigation.
	+ In response to a court order granted to individuals or their legal representatives.

Requests by the police should be made formally using a police request form. Any uncertainty regarding the validity of a request should be raised with the DPO.

Any person whose image has been recorded has a right to access the footage which relates to them as part of a Subject Access Request (SAR). Any person or organisation making a request for access to personal data (images / video footage) should provide information, such as the date, time and location of the recording to help Organisation name find the recorded data. Organisation name will follow the organisation’s SAR policy that is described at the Organisation name’s Data Protection Policy.

Importantly, where the image/recording identifies another individual(s), those images may only be released if they can be redacted/anonymised or with the explicit consent of the other people identifiable in the footage.

Depending on circumstances, Organisation name may provide a data subject a copy of their data in the form of a still image / series of still images or as a video on a tape, disk or digital media (SDD).

# Responsibilities

## Councilors and employees

The roles and responsibilities of employees responsible for the operation and management of the CCTV and associated technologies should be defined. Similarly, the responsibility of councilors for oversight of the CCTV system should be defined.

## Contractors

The council’s CCTV system is controlled by a contracted security company.

The following applies:

Organisation name has a written contract with the security company in place which details the areas to be monitored, how long data is to be stored, what the security company may do with the data, what security standards should be in place and what verification procedures apply.

The written contract also states that the security company will give the council all reasonable assistance to deal with any subject access request made under data protection laws which may be received by Organisation name within the statutory timeframe (generally 30 days).

Security companies that place and operate cameras on behalf of clients are considered to be ‘Data Processors’. As data processors, they operate under the instruction of data controllers (their clients).

Data protection laws place several obligations on data processors. These include having appropriate security measures in place to prevent unauthorised access to, or unauthorised alteration, disclosure, or destruction of, the data, where the processing involves the transmission of data over a network and against all unlawful forms of processing.

This obligation can be met by having appropriate access controls to image storage or having robust encryption where remote access to live recording is permitted. The contractor should have been made aware of their obligations relating to the security of data. As part of their annual review of the CCTV system, the data controller/councillors should seek assurance that these obligations are being met by the contractor.]

# Implementation and Review

The policy will be reviewed biennially or in the event of significant change to the system, national guidance, best practice of legislation relating to the capture of images by CCTV.

This policy was approved by the Council on date

Signed: NAME & ROLE