

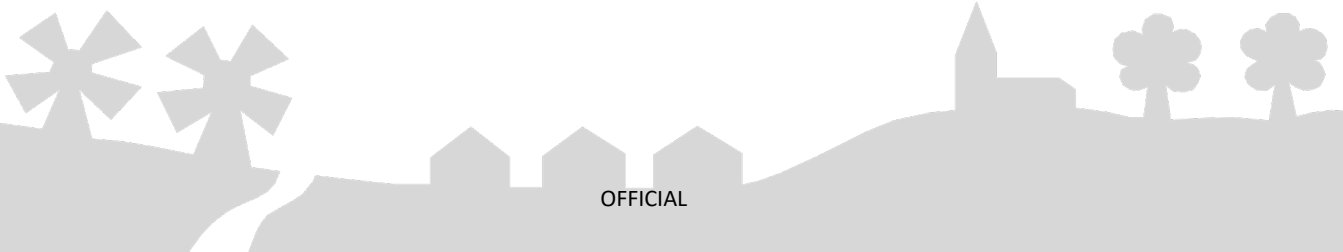


# CCTV Policy

---

**Official**

**August 2024**



# Introduction

Closed Circuit Television (CCTV) is used by Mid Sussex District Council at some of its properties and in the high streets of the three main towns in the district. The Council acts as data controller for the CCTV systems it operates.

The purpose of these systems is to:

- monitor security of premises
- reduce the fear of crime and anti-social behaviour
- apprehend and prosecute offenders; and
- prevent and detect crime

Images are recorded but are not monitored in real-time. Relevant signs are in place informing people that they are being recorded and who to contact if they have any queries or would like to request a copy.

## 1. Legislation governing use of CCTV

The CCTV systems in place will be operated in accordance with the requirements of the following legislation:

- UK General Data Protection Regulation
- Data Protection Act 2018
- Protection of Freedoms Act 2012
- Regulation of Investigatory Powers Act 2000 (where this is relevant)
- Human Rights Act 1998

We will also operate all CCTV in accordance with the principles set out in the Surveillance Camera Code Of Practice. CCTV shall be operated with due regard to the principle that everyone has the right to respect his or her private and family life and home. Public interest in the operation of CCTV will be recognised by ensuring the security and integrity of operational procedures which sit underneath it, and which balance the objectives of CCTV usage with the need to safeguard the individual's rights.

## 2. Scope

This policy applies to all overt (open) CCTV installations controlled by the council, including both internal and external cameras. It does not cover Body Worn Cameras (BWC), which are covered under a separate policy. This policy should be read in conjunction with the CCTV procedural guidance.

## 3. What areas are covered by the cameras?

### Oaklands Offices

31 cameras on site:

- **External:** Various cameras covering Car Parks, Campus and Ground Floor Building Exits

- **Internal:** Various cameras covering Reception and Main Entrances into the building

## **Orchards Shopping Centre**

19 cameras on site:

- **External:** Various cameras covering the main thoroughfares in the Orchards.
- **Internal:** (Centre Manager's Office).

## **Martlets Car Park**

5 Cameras on site.

## **Town Centre CCTV**

### **Burgess Hill Town Centre and St John's Park**

8 cameras.

### **East Grinstead Town Centre and Kings Centre**

17 cameras.

### **Haywards Heath Town Centre, Clair Park and Victoria Park**

7 cameras

## **Redeployable CCTV**

Mid Sussex District Council are responsible for the management of two redeployable CCTV cameras which were purchased through the Mid Sussex Partnership (MSP). Locations are agreed through the multi-agency Community Safety Sub-Group which reports to the MSP. The cameras are only used in public spaces where there is evidence of crime or anti-social behaviour, and signage will be clearly displayed in each location where the cameras are deployed.

## **4. Management of the system**

All staff with operational access to CCTV equipment are responsible for following the specific operational procedures established for its use. This includes checking the equipment and reporting to management where it is found to deviate from the agreed specification or appears to have been interfered with.

Staff, contractors and other relevant persons shall only be permitted access to images obtained via CCTV on a 'need to know' basis.

**Oaklands** - Day-to-day operational responsibility rests with the Information Manager. Any breaches of this policy will be reported to the Assistant Director, Digital and People Services

**Orchards Shopping Centre** - Day-to-day operational responsibility rests with the Orchards Centre Manager. Any breaches of this policy will be reported to the Information Manager, MSDC. Orchards

Security Staff, supplied by Pagoda, are certified to use the software on behalf of the Orchards Centre Manager.

**Redeployable CCTV** - Day-to-day operational responsibility rests with the Community Safety and Safeguarding Manager. Any breaches of this policy will be reported to the Information Manager.

**Town Centre CCTV** – Day-to-day operational responsibility rests with the Information Manager. Sussex Police will have also access to the town centre CCTV for tackling and responding to crime and disorder issues. Police can access any of the CCTV cameras from within their local and regional operational control rooms with priority access should a serious incident occur. Sussex Police have secure viewing procedures and must also comply with the council's procedures and protocols. Any breaches of this policy will be reported to the Assistant Director, Digital and People Services.

All staff actions, which affect the operation of the CCTV equipment should be captured in audit logs held on the devices or controlling applications. This includes any actions which change the field of vision, any downloads of footage and any deletion of footage.

Recordings will be stored on secure Council-approved devices. Any data downloaded by Sussex Police will be stored on their own secure system.

## 5. Regulation of Investigatory Powers (RIPA)

Targeted, covert (secret) surveillance of individuals will only be undertaken for good reason, and in line with the procedures set out in the Regulation of Investigatory Powers Act (RIPA) Policy. Local authorities can only authorise the use of directed surveillance under RIPA to prevent or detect criminal offences that are punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months imprisonment. Applications to carry out directed surveillance can only be made by the senior authorising officer of those public authorities listed in or added to Section 32(6) of the 2000 Act. Within the Police, such authority sits with designated senior officers.

The viewing of everyday CCTV footage is not considered to be covert recording and is therefore covered by this policy and outside of the RIPA process. This is due to the camera being in plain sight for individuals to see and appropriate signage being in place. If a decision is made to monitor a particular employee or member of the public, this is considered to be targeted surveillance, which falls under RIPA (Regulation of Investigatory Powers Act 2000).

Moving or zooming CCTV towards individuals and their activities would be considered covert surveillance and fall outside of this policy and into RIPA unless criminal activity or public safety issues are already taking place, and cameras are moved or zoomed in response to this. A comprehensive incident log must be maintained giving a reason for the monitoring of the individual. All operators and duly authorised officers must be able to justify their actions at all times.

## 6. How long are the recordings kept?

Recordings will only be retained by the Council for a maximum of 30 days. Recordings required as evidence will be kept for a maximum of 6 months or until the evidence is no longer required, whichever is longer. Data downloaded by Sussex Police will be kept in accordance with their policies. A record or audit trail will be kept detailing how any information required by the police or as evidence in court has been handled.

Recordings will only be viewed by authorised Council personnel in the following situations

- An aggressive or abusive incident involving staff which needs to be investigated further or reported to the police
- An aggressive, criminal or abusive incident in the Orchards which needs to be investigated further or reported to the police
- A member of the public has requested a copy of the recording that was made of them.
- CCTV footage is required as evidence for example, for court or an insurance company.

In such cases, the reasons must be recorded.

## 7. Can the cameras look at neighbouring properties?

Wherever possible, cameras should be sited so that neighbouring properties cannot be overlooked and/or images recorded. Similarly, the movement of motorised cameras is restricted to prevent neighbouring properties from being overlooked.

## 8. Requests for copies of footage?

Advice and Guidance about CCTV Requests can be sought by viewing the website at: <https://www.midsussex.gov.uk/about-us/your-data/>.

**Public:** Any request for CCTV footage or images at The Orchards or Oaklands Campus should be made, by them, in writing at [dataprotection@midsussex.gov.uk](mailto:dataprotection@midsussex.gov.uk) or by using the [Subject Access Request – CCTV form](https://www.midsussex.gov.uk/about-us/your-data/) available on the website at: <https://www.midsussex.gov.uk/about-us/your-data/>.

If a member of the public has experienced a crime they should report this to the Police in the first instance, acquiring a Crime Reference number. The request for images will then come from the Police.

**Police:** For town centre cameras the Police will have the ability to download data they have viewed themselves and this data will be handled in accordance with their policies once downloaded to their system. For data relating to cameras that are not town centre cameras, the police will need to request to view CCTV footage. As a minimum, the police must have an incident number from a reported incident. The police will use a specific request form when they require downloaded copies.

**Insurance Companies/Solicitors:** Can request footage from the Council by following the guidance on the website at: <https://www.midsussex.gov.uk/about-us/your-data/>. These requests may incur a fee.

**Staff:** Staff, including Managers at any level, are not allowed to view CCTV images, without authorisation. If a member of staff believes there has been an incident e.g. someone has damaged

their car at the Oaklands car park, please direct them to fill in the CCTV authorisation form which must be sent to the Information Manager who will look into the case and determine if any images can be released.

All completed authorisation forms are to be retained securely.