



Hurstpierpoint & Sayers Common Parish Council  
Email: [office@hurstpierpoint-pc.gov.uk](mailto:office@hurstpierpoint-pc.gov.uk)  
Website: [www.hurstpierpoint-pc.gov.uk](http://www.hurstpierpoint-pc.gov.uk)  
Telephone: 01273 833264

Village Centre  
Trinity Road  
Hurstpierpoint  
West Sussex BN6 9UY

# CCTV Policy

Presented to Council 14 December 2023

## Introduction

The Hurstpierpoint & Sayers Common Parish Council uses closed circuit television (CCTV) images to protect the Parish Council's premises at Court Bushes Community Hub, Willow Way, Hurstpierpoint. This Policy sets out the details of how the Parish Council will collect, use and store CCTV images. For more information on your privacy rights associated with the processing of your personal data collected through CCTV images please refer to the Parish Council privacy notice and Data Protection Policy.

## Purposes of CCTV

The Parish Council has carried out a data protection impact assessment (Appendix A) and on the basis of its findings it considers it necessary and proportionate to install and use a CCTV system. The data collected from the system will assist in:

- Prevention or detection of crime or equivalent malpractice.
- Identification and prosecution of offenders.
- Monitoring of security of the Parish Council's premises.

## Location of cameras

Cameras are located at strategic points around Court Bushes Community Hub, principally covering entrances and exits to the building. The Parish Council has positioned the cameras to only cover public areas into and around the building and they have been sited so that they provide clear images. No camera focuses, or will focus, on toilets, staff kitchen areas, staff break rooms or private offices.

All cameras (with exception of any that may be temporarily set up for covert recording) are also clearly visible.

Appropriate signs are prominently displayed so that employees, clients, customers, and other visitors are aware they are entering an area covered by CCTV.

## Recording and retention of images

Images produced by the CCTV equipment are intended to be as clear as possible so that they are effective for the purposes set out above. Maintenance checks of the equipment are undertaken on a regular basis to ensure it is working properly and that the media is producing high quality images.

Images may be recorded either in constant real-time (24 hours a day throughout the year), or only at certain times, as the cameras detect movement on the premises.

As the recording system records digital images, any CCTV images that are held on the hard drive of a PC or server are deleted and overwritten on a recycling basis and, in any event, once the hard drive has reached the end of its use, it will be erased prior to disposal.

Images that are stored on, or transferred on to, removable media such as CDs or which are stored digitally are erased or destroyed once the purpose of the recording is no longer relevant. In normal circumstances, this will be a period of 12 months. However, where a law enforcement agency is investigating a crime, images may need to be retained for a longer period.

### **Access to and disclosure of images**

Access to, and disclosure of, images recorded on CCTV is restricted. This ensures that the rights of individuals are retained. Images can only be disclosed in accordance with the purposes for which they were originally collected.

The images that are filmed are recorded centrally and held in a secure location. Access to recorded images is restricted to the operators of the CCTV system and to those line managers who are authorised to view them in accordance with the purposes of the system. Viewing of recorded images will take place in a restricted area to which other employees will not have access when viewing is occurring. If media on which images are recorded are removed for viewing purposes, this will be documented.

Disclosure of images to other third parties will only be made in accordance with the purposes for which the system is used and will be limited to:

- The Police and other law enforcement agencies, where the image recorded could assist in the prevention or detection of a crime or the identification and prosecution of an offender or the identification of a victim or witness.
- Prosecution agencies, such as the Crown Prosecution Service.
- Relevant legal representatives.
- Individuals whose images have been recorded and retained (unless disclosure would prejudice the prevention or detection of crime or the apprehension or prosecution of offenders).

The Chairman of the Parish Council or Clerk to the Council are the only people who are permitted to authorise disclosure of images to external third parties such as law enforcement agencies.

All requests for disclosure and access to images will be documented, including the date of the disclosure, to whom the images have been provided and the reasons why they are required. If disclosure is denied, the reason will be recorded.

### **Individuals access rights**

Under the UK's data protection laws, including the General Data Protection Regulations (GDPR), individuals have the right on request to receive a copy of the personal data that the Parish Council holds about them, including CCTV images if they are recognisable from the image.

If an individual wishes to access any CCTV images relating to them, they must make a written request to the Clerk to the Council in writing or by emailing [office@hurstpierpoint-pc.gov.uk](mailto:office@hurstpierpoint-pc.gov.uk). The Parish Council will usually not make a charge for such a request but may charge a reasonable fee if a request is made which is manifestly unfounded or excessive or is repetitive. The request must include the date and approximate time when the images were recorded and the location of the particular CCTV camera, so that the images can be easily located, and that their identity can be established as the person in the images.

The Parish Council will usually respond promptly and in any case within one month of receiving a request. However, where a request is complex or numerous the Parish Council may extend the one month to respond by a further two months.

The Clerk to the Council will always determine whether disclosure of the images will reveal third party information, as an individual has no right to access CCTV images relating to other people. In this case, the images of third parties may need to be obscured if it would otherwise involve an unfair intrusion into their privacy.

If the Parish Council is unable to comply with a request because access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders, the individual will be advised accordingly.

### **Covert recording**

The Parish Council is aware that covert recording can only be done in exceptional circumstances for example where the Parish Council suspects criminal activity taking place. On this basis the Parish Council will only undertake covert monitoring if it has carried out a further data protection impact assessment which has addressed the following:

- The purpose of the covert recording.
- The necessity and proportionality of the covert recording.
- The risks to the privacy rights of the individual(s) affected by the covert recording.
- The time parameters for conducting the covert recording.
- The safeguards and/or security measures that need to be put in place to ensure the covert recording is conducted in accordance with the data protection laws, including the GDPR.

If after undertaking the data protection impact assessment the Parish Council considers there is a proportionate risk of criminal activity, or equivalent malpractice taking place or about to take place, and if informing the individuals concerned that the recording is taking place would seriously prejudice its prevention or detection, the Parish Council will covertly record the suspected individual(s). In doing this the Parish Council will rely on the protection of its own legitimate interests as the lawful and justifiable legal basis for carrying out the covert recording.

Before the covert recording commences the Parish Council will ensure that Chairman of the Parish Council (or another Councillor acting in their absence) agrees with the findings of the data protection impact assessment and provides written authorisation to proceed with the covert recording. Covert monitoring may include both video and audio recording.

Covert monitoring will only take place for a limited and reasonable amount of time consistent with the objective of assisting in the prevention and detection of particular suspected criminal activity or equivalent malpractice. Once the specific investigation has been completed, covert monitoring will cease.

Information obtained through covert monitoring will only be used for the prevention or detection of criminal activity or equivalent malpractice. All other information collected in the course of covert monitoring will be deleted or destroyed unless it reveals information which the Parish Council cannot reasonably be expected to ignore.

### **Staff training**

The Parish Council will ensure that all employees handling CCTV images or recordings are trained in the operation and administration of the CCTV system and on the impact of the laws regulating data protection and privacy with regard to that system.

### **Implementation**

The Clerk to the Council is responsible for the implementation of and compliance with this policy and the operation of the CCTV system and will conduct a regular review of the Parish Council's use and processing of CCTV images and ensure that at all times it remains compliant with the laws regulating data protection and privacy. Any complaints or enquiries about the operation of the Parish Council's CCTV system should be addressed to the Clerk to the Council.

## **Data Protection**

The Parish Council will process the personal data collected in connection with the operation of the CCTV policy in accordance with its data protection policy and any internal privacy notices in force at the relevant time.

Inappropriate access or disclosure of this data will constitute a data breach and should be reported immediately to the Clerk to the Council in accordance with the Parish Council's data protection policy.

Reported data breaches will be investigated and may lead to sanctions under the Parish Council's disciplinary procedure.

## Appendix A

# Data Protection Impact Assessment for CCTV Usage

---

### Step 1: Identify the need for a DPIA

**Explain broadly what project aims to achieve** and what type of processing it involves. You may find it helpful to refer to or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Due to an increase of anti-social behaviour (ASB) at Court Bushes Community Hub, Willow Way during September, October and November 2023, it was made apparent that the existing CCTV camera on site were not effective to capture the recent ASB events, including the breaking of 14 lit bollards, the breaking of a light cover on the outside of the building and the smashing of a window at the rear of the building (nursery). The only footage captured was of potential suspects, and the destruction of carved pumpkins in the lead up to Halloween.

The aim of the CCTV cameras, with 3K resolution and motion activated white lights, which will provide full colour images in day or night conditions, to be placed in key locations around the building to cover blind spots, including the main driveway (location of bollard damage), the front entrance and bin area and the rear car park and nursery.

### Step 2: Describe the processing.

**Describe the nature of the processing:** how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

The CCTV cameras will record footage only when it detects movement on our premises, the footage will be uploaded to a cloud storage and is only accessible through the Mobile App on the Clerk's mobile phone or onsite in the Court Bushes Community Hub office. All data is password protected and only authorised staff will be able to view the footage.

Footage will only be viewed in the event of an incident, i.e., ASB, vandalism, unreported damage and reported damage (if the event is needed to be confirmed for insurance purposes).

All footage held in the cloud storage will automatically be deleted and overwritten after 1 month.

Any footage that captures relevant events will be downloaded to the ASB folder in the Parish Council's SharePoint and this data will be only shared with authorisation from the Chairman of the Parish Council or the Clerk and will only be supplied to Sussex Police and the ASB team at Mid Sussex District Council.

**Describe the scope of the processing:** what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

The data collected is in video (no audio) and images, any movement activates the camera to record, the cameras may collect from 3 to 50 recordings a day depending on activity at the site. Usually, this footage will not be viewed unless there is a corresponding event which requires additional evidence to be captured.

Footage and images may only be viewed and used once a month or a couple of times a year at most.

All footage not used will be deleted and overwritten after 1 month, any footage or images downloaded and shared, will be retained for 3 months. If they are being used for a criminal conviction this can be extended as required.

The CCTV cameras cover the area around the outside of the Court Bushes Community Hub.

### Step 3: Consultation process

**Consider how to consult with relevant stakeholders:** describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

We have consulted with Hallmark Security our present security contractor, who is responsible for maintaining the existing CCTV system.

In the event of video footage being download for sharing with Sussex Police and ASB teams, either the Chair of the Parish Council or the Clerk will be consulted to authorise the sharing of these images or footage.

### Step 4: Identify and assess risks

| <b>Describe source of risk and nature of potential impact on individuals.</b> Include associated compliance and corporate risks as necessary. | <b>Likelihood of harm</b> | <b>Severity of harm</b> | <b>Overall risk</b> |
|-----------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|-------------------------|---------------------|
| <b>Risk:</b><br>Images are leaked to the public.                                                                                              | Low                       | Minimal                 | Low                 |
| <b>Impact on individuals:</b><br>Embarrassment/pride in being identified as suspect.                                                          | Low                       | Minimal                 | Low                 |

**Step 5: Identify measures to reduce risk.**

| <b>Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5</b> |                                            |                       |                      |                         |
|-----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|-----------------------|----------------------|-------------------------|
| <b>Risk</b>                                                                                                                 | <b>Options to reduce or eliminate risk</b> | <b>Effect on risk</b> | <b>Residual risk</b> | <b>Measure approved</b> |
| Not applicable.                                                                                                             | Not applicable.                            |                       |                      |                         |

**Step 6: Sign off and record outcomes.**

| <b>Item</b>                           | <b>Name/date</b>                    | <b>Notes</b>                                                                          |
|---------------------------------------|-------------------------------------|---------------------------------------------------------------------------------------|
| Measures approved by:                 | Sarah Groom<br>Clerk to the Council | Integrate actions back into project plan, with date and responsibility for completion |
| Residual risks approved by:           | Sarah Groom<br>Clerk to the Council | If accepting any residual high risk, consult the ICO before going ahead               |
| DPO advice provided:                  | Not applicable.                     | DPO should advise on compliance, step 6 measures and whether processing can proceed   |
| Summary of DPO advice: Not applicable |                                     |                                                                                       |
| DPO advice accepted or overruled by:  | Not applicable                      | If overruled, you must explain your reasons                                           |
| Comments: Not applicable              |                                     |                                                                                       |
| Consultation responses reviewed by:   | Not applicable                      | If your decision departs from individuals' views, you must explain your reasons       |
| Comments: Not applicable              |                                     |                                                                                       |
| This DPIA will kept under review by:  | Sarah Groom<br>Clerk to the Council | The DPO should also review ongoing compliance with DPIA                               |