

# CCTV and Surveillance Camera Policy

<b>Author</b>	<b>Kathy Fowler, Prevention and Enforcement Service Manager, Prevention &amp; Enforcement</b>
<b>Approved by</b>	<b>Cabinet</b>
<b>Approval date</b>	<b>April 2025</b>
<b>Review date</b>	<b>March 2027</b>

## 1. Policy Summary

- 1.1 Havant Borough Council (the Council) in the 2024 – 2028 Corporate Strategy outlined a political imperative to design and implement a new preventative enforcement approach. Our residents stated that feeling safe is the 2nd top priority for them, with litter and fly-tipping joint 3rd, vandalism and graffiti 4th and cleaner streets 5th. Focusing on these top 5 areas of concern we aim to improve the quality of place across the Borough, address long standing issues and, where necessary, consider Closed Circuit Television [CCTV], (and other surveillance, including Dash Cameras, and Body Worn Video [BWV]) installation to improve all areas of concern to help improve the safety and quality of place.
- 1.2 The Council already has in place CCTV and other surveillance systems. This policy details the purpose, use, and management of the systems, and details the procedures to be followed to ensure that the Council complies with relevant legislation and Codes of Practice where necessary.
- 1.3 This policy and the procedures therein detailed, applies to all the Council's CCTV and surveillance systems, including overt and covert installations, static and re-deployable cameras capturing images of identifiable individuals for the purpose of viewing, and / or recording the activities of such individuals.
- 1.4 CCTV and surveillance system images are monitored and recorded in strict accordance with this policy.

## 2. Introduction

- 2.1 The Council uses CCTV and surveillance system images for the prevention and detection of crime, public safety, anti-social behaviour, and waste crime (to include fly-tipping, fly-posting



# CCTV and Surveillance Camera Policy

and litter enforcement) to monitor the Council's buildings and land to provide a safe and secure environment for staff, volunteers, contractors, and visitors, and to prevent the loss of or damage to the Council's contents and property.

- 2.2 The CCTV and surveillance systems are owned by the Council and managed by the Council and / or its appointed agents. The Council is the system operator, and data controller, for the images produced by the CCTV and surveillance systems, and is registered with the Information Commissioner's Office, Registration number Z5747526.
- 2.3 This policy applies to CCTV and other surveillance camera devices that view or record individuals.
- 2.4 This policy uses the terms 'surveillance system(s)', 'CCTV' and 'information' throughout for ease of reference, and would include (but is not limited to) the following types of systems:
  - 2.4.1 Fixed CCTV (networked)
  - 2.4.2 Body Worn Video BWV
  - 2.4.3 Unmanned aerial systems (drones)
  - 2.4.4 Stand-alone cameras
  - 2.4.5 Re-deployable CCTV
  - 2.4.6 Dash Cameras

### 3. Purpose

- 3.1 This Policy governs the installation and operation of all CCTV and surveillance systems at the Council and within the Borough.
- 3.2 CCTV surveillance is used to monitor and collect visual images for the following purposes.
  - a) To help reduce the fear of crime to provide a safe and secure environment for residents of, and visitors to, the areas covered by the scheme.
  - b) To help deter and detect crime and provide evidential material for court proceedings.
  - c) To help deter and detect anti-social behaviour, including fly-tipping and litter enforcement and provide evidential material for the issuing of Fixed Penalty Notices [FPN] and Penalty Notices [PN] and or court proceedings.
  - d) To assist in the overall management of the Council.



# CCTV and Surveillance Camera Policy

- e) To assist in the management of other locations and buildings owned or controlled by the Council.
- f) To enhance community safety, including the prevention and detection of harassment, to assist in developing the economic well-being of Havant Borough and encourage greater use of the town centres.
- g) To assist the local authority in their enforcement and regulatory functions within the Havant Borough.
- h) To assist in supporting civil proceedings.
- i) To assist the Council in discharging its health and safety obligations towards staff.
- j) To investigate allegations of staff misconduct.

## 4. Scope

- 4.1 This policy applies to all CCTV and related surveillance systems operated by the Council.
- 4.2 Where a system is jointly owned or jointly operated, the governance and accountability arrangements are agreed between the partners and documented so that each of the partner organisations has clear responsibilities, with clarity over obligations and expectations and procedures for the resolution of any differences between the parties or changes of circumstance.
- 4.3 This policy is applicable to, and must be followed by, all staff including consultants, partners and contractors. Failure to comply could result in disciplinary action, including dismissal. This policy also applies to volunteers and Councillors.
- 4.4 All staff involved in the operation of the CCTV System will be made aware of this policy and will only be authorised to use the CCTV System in a way that is consistent with the purposes and procedures contained therein.
- 4.5 All systems users with responsibility for accessing, recording, disclosing or otherwise processing CCTV images will have relevant skills and training on the operational, technical and privacy considerations, and fully understand the policies and procedures.

## 5. Policy Statement

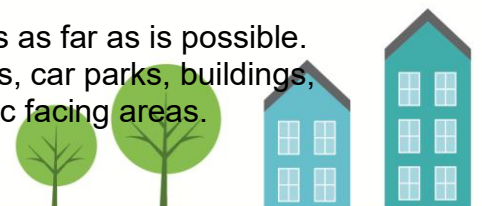


# CCTV and Surveillance Camera Policy

- 5.1 The Council will, subject to 5.5b below, operate its CCTV systems in a manner that is consistent with respect for the individual's privacy.
- 5.2 The Council complies with the Information Commissioner's Office (ICO) CCTV Code of Practice and The Surveillance Camera Code of Practice, introduced under the Protection of Freedoms Act 2012, which provides 12 guiding principles for the lawful, transparent, and proportionate use of surveillance systems (CCTV, ANPR, Body Worn Video) to ensure that surveillance is used responsibly and safeguards both trust and confidence in its continued use.
- 5.3 The use of the CCTV systems will be conducted in a professional, ethical, and legal manner, and any diversion of the use of CCTV security technologies for other purposes is prohibited by this policy.
- 5.4 Cameras will be sited so they only capture images relevant to the purposes for which they are installed. In addition, equipment must be carefully positioned to:
  - a) cover the specific area to be monitored only.
  - b) keep privacy intrusion to a minimum.
  - c) ensure that recordings are fit for purpose and not in any way obstructed (e.g. by foliage).
  - d) minimise risk of damage or theft.
- 5.5 CCTV Cameras will not be used for monitoring audio conversations or be used to talk to individuals. BWV are excluded from this.
- 5.6 Before any CCTV system is installed, service areas will have considered other, less intrusive methods to achieve the objectives of having a CCTV system in place (e.g. improving lighting in an area to prevent crime).
- 5.7 In the ordinary course of business, cameras will not usually be used to monitor the progress of staff or individuals in the area under surveillance. Managers are not usually permitted to use the cameras to observe staff working practices or time keeping or to assist them in the day-to-day management of their staff without prior approval from HR and usually as part of an investigation.

## 6. Location and signage

- 6.1 Cameras are sited to ensure that they cover the relevant areas as far as is possible. Cameras are installed throughout the site/s including roadways, car parks, buildings, premises, within buildings and vehicles, and externally in public facing areas.

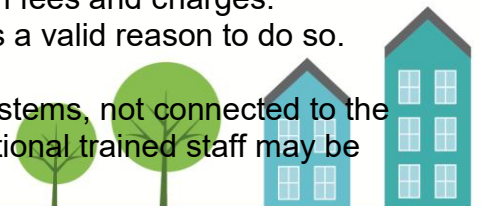


# CCTV and Surveillance Camera Policy

- 6.2 The location of equipment is carefully considered to ensure that images captured comply with data protection requirements. Every effort is made to position cameras so that their coverage is restricted to the relevant area, which may include outdoor public spaces and recreational areas.
- 6.3 Signs are placed wherever CCTV systems are in operation, to inform individuals that CCTV is in operation.
- 6.4 When officers are wearing Body Worn Video Cameras they will wear a badge informing the public of this.
- 6.5 The signage indicates that monitoring and recording is taking place, for what purposes, who the system owner is (if it is not obvious), and where complaints / questions about the systems should be directed.
- 6.6 Where Dash Cameras are fitted to HBC logo vehicles there will be signage that indicates that monitoring and recording is taking place for the detection of crime waste and may record when stationary to detect any vandalism to HBC vehicles.

## 7. Monitoring and recording

- 7.1 The casual review or trawling of recorded images by anyone is strictly forbidden. Reviews must only be undertaken for a specific, legitimate purpose.
- 7.2 Cameras are monitored in a secure private offices and locations. For business continuity IT devices that have camera monitoring installed maybe used off site but in secure and private locations and cannot be overviewed by others. All users will adhere to The Council's ICT Security Responsibilities policy.
- 7.3 System administrators can view and access footage for the purposes for which the CCTV system is in operation. Before any further disclosure is made (e.g. to an external organisation, or another internal department / member of staff), agreement and co-operation should be sought from the Data Protection Officer.
- 7.4 The management of the cameras (to include repositioning of the cameras and the viewing position) is the responsibility of trained HBC personnel only. HBC can instruct the supplier to reposition cameras with 24 hours' notice and agreed relocation fees and charges. Repositioning of the cameras will only be considered if there is a valid reason to do so.
- 7.5 Images are recorded on secure servers (ideally standalone systems, not connected to the network) and are viewable by the system administrators. Additional trained staff may be



# CCTV and Surveillance Camera Policy

authorised by the system administrator to access images from cameras sited within their own areas of responsibility.

- 7.6 Any staff who have access to the system are made aware of their roles and responsibilities relating to the system by the system administrator, who will also provide them with the necessary skills and knowledge to use and manage the system.
- 7.7 Staff who have access to the system will receive continued training as needed, to ensure their competence relating to relevant operational, technical, privacy considerations, policies, and procedures.
- 7.8 Where service areas are using Cloud-based storage, they will ensure that such storage is in the UK or European Economic Area (EEA), and that all relevant security and data protection measures are in place.
- 7.9 Recorded material will be stored in a way that maintains the integrity of the image and information to ensure that metadata (e.g. time, date, and location) is recorded reliably, and compression of data does not reduce its quality.
- 7.10 Viewing devices should be password protected and switched off / locked and kept in a secure place when not in use to prevent unauthorised use or viewing.
- 7.11 When viewing footage for evidentiary purposes this should be done by agreed trained personnel only. Footage should only be viewed in a secure location that cannot be overlooked by others. Viewing devices will not be removed from the offices unless previously agreed by the Service Manager and when there is a business need to do so, or in line with the service's business continuity policy. At no time shall the device be taken out of the UK or viewed in an undisclosed location.
- 7.12 The cameras installed provide images that are of suitable quality for the specified purposes for which they are installed, and all cameras are checked regularly to ensure that the images remain fit for purpose, and that the date and time stamp recorded on the images is accurate.

## 8. Covert Surveillance

- 8.1 Covert surveillance is the use of hidden cameras or equipment to observe and / or record the activities of a subject which is carried out without their knowledge.
- 8.2 The use of covert cameras or recording / monitoring will be restricted to rare occasions, in accordance with the Council's RIPA Corporate Surveillance Policy.



# CCTV and Surveillance Camera Policy

## 9. Data Protection Impact Assessments

- 9.1 In its administration of its CCTV systems, the Council complies with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and in accordance with its own Data Protection Policy.
- 9.2 The Council's CCTV systems (new and existing) are subject to a Data Protection Impact Assessment [DPIA], identifying risks related to the installation and use of the system, ensuring full compliance with the data protection principles. This will include consultation with relevant internal and external stakeholders.
- 9.3 Once systems are operational, system administrators will conduct regular reviews of the DPIA for their system.

## 10. Subject Access Requests

- 10.1 Requests by individual data subjects for images relating to themselves via a Subject Access Request [SAR] should be submitted to the Data Protection Officer at [dp@havant.gov.uk](mailto:dp@havant.gov.uk). Further details of this process are detailed on the council's website. Also on this webpage is a [guide](#) to subject access rights detailing all your subject access rights.
- 10.2 To locate the images on the system, sufficient detail must be provided by the data subject to allow the relevant images to be located and the data subject to be identified.
- 10.3 Where the Council is unable to comply with a Subject Access Request without disclosing the personal data of another individual who is identified or identifiable from that information, it is not obliged to comply with the request unless satisfied that the individual has provided their express consent to the disclosure, or if it is reasonable, having regard to the circumstances, to comply without the consent of the individual.
- 10.4 A search request should specify reasonable accuracy i.e. within 30 minutes.
- 10.5 A request for images made by a third party should be made to the Data Protection Officer at [dp@havant.gov.uk](mailto:dp@havant.gov.uk). Further details of this process are detailed are on [the Council's website](#).

## 11. Insurance Claims

- 11.1 CCTV involvement in insurance claims falls into two categories. Firstly, incidents, which may result in claims against the council and secondly claims involving third parties, normally road traffic collisions.



# CCTV and Surveillance Camera Policy

- 11.2 CCTV cameras may be able to assist in events that could result in a claim against the council. When a report is received which may result in a claim, the officer responsible for dealing with the incident should consider whether CCTV covers the area. If so, they should then ask the CCTV systems' responsible officer to hold images for that period, but this must be done within 28 days from the date of the incident. The officer dealing with the incident should then follow the procedures for review and obtaining evidence, which is set out in section 7 of this policy.
- 11.3 If evidence is issued to the officer dealing with the incident, they become responsible for the security, safety and integrity of the images. All recorded media must be stored in a secure place with access limited only to those people involved in the subsequent claim. At the end of the waiting period or after any claim has been dealt with this officer will be responsible for the destruction of the recorded media by shredding and a record in the form of a signed memo to that effect will be kept for a period of 12 months.
- 11.4 Requests for assistance from CCTV cameras in third party claims are increasing especially with regard to road traffic collisions. Often it is the person involved in the accident who will contact CCTV and ask either if we have any images or if they can come and have a look. Requests of this kind should normally be refused. Instead, members of the public should be advised to contact their insurance company and ask them to write to the responsible officer formally, giving as much detail about the incident as possible and requesting assistance. It is also important that it is stressed to the person requesting the information, that the information is requested as soon as possible before the automatic overwrite/ delete period on the recorder (normally 31 days). No other action should be taken at this stage.
- 11.5 If the request arrives within the recording period, the responsible officer should view the images. If the incident was not caught on camera the insurers or solicitor can be called and informed and the case can be closed. If the letter arrives after the recording period, there will be no relevant images and again the person requesting the images should be informed.
- 11.6 If relevant images are found on the video image recorder, the insurance company/ solicitor should be informed and asked if they want a copy. If they do, then they need to be informed that there will be a fee as set out in the council's schedule of fees and charges. This fee is based on the amount of time spent by staff to review extracted the images, to copy them and for any other processing of the images together with the administration, completion of appropriate documentation, cost of media, disk labelling etc. and is based on the hourly salary rate rounded up to the nearest hour. It should also include post and packaging. This should then be sent as an invoice to the recipient. No charges will be raised against internal requests for assistance.



# CCTV and Surveillance Camera Policy

11.7 The images may then be copied and sent to the relevant person accompanied by two copies of a letter reminding them that the council retains 'copyright' over the images, that they are responsible for the security and destruction of the images and that the images may not be used for any other purpose other than the one they were released for. The details of the media released should be included (i.e. media number) in the letter and they should be asked to sign one copy of the letter confirming they have received the images and accepting the conditions of release. A detailed record of all actions must be maintained. Failure to comply with the conditions of release may result in legal action being taken against the person who signed the acceptance letter.

## 12. Third Party Disclosures

12.1 In limited circumstances it may be appropriate to disclose images to a third party, such as when a disclosure is required by law, in relation to the prevention or detection of crime or in other circumstances where an exemption applies under relevant legislation. Enforcement Agencies should provide a Crime or Incident number or other such proof that they are conducting a legitimate investigation.

12.2 Such disclosures will be made at the discretion of the system administrator, with reference to relevant legislation, and following advice from the Data Protection Officer.

12.3 Before disclosing any footage, consideration should be given to whether (if possible) images of third parties should be obscured to prevent unnecessary disclosure.

12.4 Where information is disclosed, the disclosing officer must ensure information is transferred securely, and the following instructions on the use of the images given to the recipient:

*"Once Havant Borough Council has disclosed this footage to you, you become the data controller for the copy held by you. It is your responsibility to comply with data protection legislation in relation to any further disclosures or processing. Representations from Havant Borough Council should be sought before further disclosure is made".*

## 13. Requirement to Give Evidence

13.1 All CCTV staff will be required to cooperate with Law enforcement agencies and appear in court when requested to do so.

## 14. Retention



# CCTV and Surveillance Camera Policy

- 14.1 Unless required for evidentiary purposes, the investigation of an offence, or as required by law, CCTV images will be retained for no longer than 31 calendar days from the date of recording. Images will be automatically overwritten or destroyed after this time.
- 14.2 Any footage downloaded and retained for evidential purposes must be reviewed after three months by the system administrator, and either a destruction date or review date must be set, with written justification for further retention recorded.
- 14.3 CCTV disclosure logs should be kept for 6 years.

## 15. Complaints Procedure

- 15.1 Complaints concerning the Council's use of its CCTV systems, or the disclosure of CCTV images should be made in the first instance to Customer Services. The contact details will be found on the signage for the relevant system.
- 15.2 For complaints where contact details can't be identified, these should be made to the Council's Data Protection Officer ([dp@havant.gov.uk](mailto:dp@havant.gov.uk)).
- 15.3 Depending on the nature of the complaint, it will either be processed under the Council's Corporate Complaints process, or (more likely) treated as a data protection concern to be investigated by the Council's Data Protection Officer.

## 16. Management

- 16.1 This Policy is reviewed every two years or sooner should changes be required and is approved by Cabinet. The Council's Information Governance Steering Group has oversight of this policy, and the Head of Compliance has been identified as its CCTV Senior Responsible Officer for Surveillance Systems (SRO).
- 16.2 The SRO has strategic responsibility for the integrity and efficacy of the processes in place within the Council that ensure compliance with the Protection of Freedoms Act 2012, and in respect of all surveillance camera systems operated by the Council.
- 16.3 The SRO is supported by the Prevention and Enforcement Service Manager whose team administers the CCTV systems at an operational level. The SRO and the Prevention and Enforcement Service Manager will work together to ensure this policy is implemented across the authority.



# CCTV and Surveillance Camera Policy

16.4 The Prevention and Enforcement Service Manager will monitor implementation and compliance with this policy for the systems they administer. Users found in breach of this policy may be subject to disciplinary action.

## **17. Copyright**

17.1 Copyright and ownership of all material recorded by virtue of the system will remain and owned by Havant Borough Council.



# CCTV and Surveillance Camera Policy

## 18. Appendix 1 – Types of CCTV

The following types of CCTV are used by the council:

### CCTV Cameras on the council's Civic Offices:

The use of CCTV cameras on the council's campus is currently restricted to the following areas:

Public Service Plaza entrances, exits, stairwells and public areas.

### Body Worn Video Cameras [BWV]:

BWV cameras are currently used by Prevention and Enforcement Officers, Animal Welfare when on inspections and on occasions the front-line customer service officers. Such use is intended for the safety of staff and the public as well as the reduction and detection of crime and anti-social behaviour and images may be used in evidence. Footage from these cameras may also be used for staff training and investigating complaints where necessary.

### Covert CCTV monitoring:

Any use of covert CCTV monitoring will be undertaken in accordance with the requirements set out in the Regulation of Investigatory Powers Act 2000 (RIPA). RIPA requires that due consideration is given to the proportionality and necessity of any covert activity and that regard is given to the rights of individuals under Article 8 of the Human Rights Act (the right to privacy).

### CCTV Meridian Centre and Bus Station:

There are CCTV cameras on the exits of the Meridian Centre out to the Bus Station for the purposes of reducing and detecting crime and anti-social behaviour as well as the safety of staff and visitors.

### Remotely Operated Vehicles (Drones):

The council uses drones to gather information for flood maps and flood risk situations, emergency response, severe weather, roads, and infrastructure development. The Drones are operated by the Coastal Partnership.

### Static and Redeployable Cameras within the Borough:

There are CCTV cameras in town centres, in particular specific locations in:



# CCTV and Surveillance Camera Policy

- Waterlooville Town Centre.
- Havant Town Centre.
- Greywell and Park Parade shopping precinct.
- Greywell car park, Tidworth Road car park.
- Hayling Island, Eaststoke Corner, HI Community Centre, West Beach, Chichester Avenue car park. Monitoring specific organised crime and ASB as per police intelligence and intervention.
- Emsworth – Palmers Road, and Hollybank (recycling banks in the car parks of the) Recreational ground.

Note – re-deployable cameras maybe installed at new locations for a specified time at the request of the police when enforcing dispersal orders (public disorders and the prevention and detection of crime).

Notification will be sent to the DPO as and when redeployable (solar) cameras are moved to different locations.

Dash Cam footage and litter offence - (dash cams fitted to HBC owned and branded vehicles).

Dash cam footage may be used to issue Fixed Penalty Notices [FPN] and Penalty Notices [PN] based on the video evidence that clearly shows the vehicles registration number and offence of litter being thrown out of the vehicle when using their enforcement powers under or connected to sections 87 to 88A or schedule 3A of the EPA 1990.

Liability – it is the registered keeper of the vehicle that is held liable, regardless of who threw the litter, and it will be the registered keeper who will receive the fine in the post.

Declaration of Confidentiality

All personnel and contractors to read and sign a declaration and agree to adhere to the process and policies of this document.



# CCTV and Surveillance Camera Policy

## Version control record

Version number	Date	Author / reviewer	Comments / changes
V0.1	14.02.2025	Kathy Fowler	First draft
V0.2	01.02.2025	Cheryl Lincoln	Corporate Compliance Manager & Data Protection Officer
V0.3	20.02.2025	Will Jackson	Chief Policy Officer
V0.4	15.01.2026	Kathy Fowler	Additional locations
V0.5	23.03.2026	Kathy Fowler	Additional locations

