Havering Council CCTV Policy 2026

V1.0 - 01/03/2025

CCTV Policy Table of Contents

(Page intentionally blank)

Section 1 Document Control

Date	Reason for Issue	Issued by
01/02/2025	Initial Issue	Chris McAvoy
01/03/2025	Minor Amendments	Chris McAvoy
30/05/2025	Signed off by all BPs	Chris McAvoy
24/09/2025	Addition of BWV	Mel Gadd
25/11/2025	Signed off by all BPs	Mel Gadd

Part 1 Overview

Section 2

Closed Circuit Television (CCTV) is a tool used by Havering Council to prevent and detect and reduce the fear of crime.

The Council uses Closed Circuit Television systems in many of its buildings, public spaces and car parks across the borough of Havering for public space surveillance.

For clarity, this Policy is to outline the operation of Havering Council's Public Space and Housing Estate (HRA) CCTV systems operating within the borough and details how CCTV will be used by the Council, employees, and contractors and accessed by law enforcement organisations.

This policy also sets out the framework for the use of Body Worn Video equipment by Havering staff, outlining the aims operational procedures, data handling, and individual rights associated with its use.

This policy applies to all Havering staff and authorised officers involved in the use, review, and management of BWV equipment and data. Non-compliance may result in disciplinary action.

The Council has a separate CCTV camera system for traffic enforcement. The use of CCTV cameras for traffic enforcement is regulated by the Code of Practice published by The London Councils Transport & Environment Committee and is out of scope of this Policy document.

Other standalone camera systems such as those in schools, libraries and other council buildings and depots also fall outside of the scope of this policy document.

Our CCTV Operations Policy reflects the 12 Guiding Principles listed in the **Surveillance Camera Code of Practice 2013:**

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
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.
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.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
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.
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.
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.
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.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

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.
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.
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.

Part 2 CCTV

Section 3 Council's CCTV Scheme Aim and Objectives

The following are objectives of London Borough of Havering's CCTV scheme:

- Deterring crime and assist in the detection of criminal offences
- Deterring anti-social behaviour and assist in the detection of anti-social behaviour incidents
- Reducing the fear of crime and anti-social behaviour
- Improving the safety and security of residents, visitors and the business community who use the facilities covered by the CCTV scheme.
- Assisting the emergency services in the location of missing vulnerable persons.
- CCTV evidence for police investigations and prosecutions

The Council will not use its CCTV for:

- Monitoring the activities of anyone for reasons of age, gender, religion or race and who have not come to the attention of the operators of the system for one of the above reasons:
- Monitoring anyone lawfully going about their business, unless circumstances are such that give rise to concerns for that person's safety;
- Intrude into the privacy of any individual unless in pursuit of one of the above authorised uses; and/or
- For purposes of entertainment.

The CCTV systems will not be used for any other purpose than those set out in this document without prior consultation with and the authorisation of the Executive Director of the Place department

Section 4 Ownership and Management of the CCTV System

The public space CCTV system is wholly owned by Havering Council.
The day-to-day management of the CCTV scheme is the responsibility of the service manager responsible for CCTV, supported by the CCTV Control Room team.

The Metropolitan Police South Area BCU Commander will be responsible for ensuring that all police officers and other Metropolitan Police Service employees involved in the CCTV scheme adhere to this Policy.

4.1 Senior Responsible Officer (SRO)

The Chief Executive of Havering has overall responsibility for ensuring that all CCTV systems owned by Havering Council are operated in accordance with all relevant guidance and

legislation and has been designated as the Senior Responsible Officer (SRO) as defined in guidance issued by the Surveillance Camera Commissioner.

4.2 Single Point of Contact (SPOC)

For the purposes of this policy only, Havering Council has designated the Head of Enforcement and Community Safety as the Single Point of Contact (SPOC), responsible for Public Realm and HRA CCTV.

For the purpose of parking and traffic enforcement, the Head of Community Safety shall delegate the SPOC to the Parking Enforcement Manager.

Other CCTV schemes across the council have their own local SPOCs. The SPOC's role for each system is for all operational matters relating to specific surveillance camera systems.

Each of the SPOCs will support the Chief Executive Officer (the SRO) regarding overall CCTV compliance.

The SPOCs should ensure that any staff across the Council operating surveillance cameras are properly trained, kept up to date on changes to legislation and are operating systems correctly.

Section 5 Administration and Management of the CCTV System

5.1 Contributors to the Policy

This Policy has been prepared in consultation between the Council, Metropolitan Police Service and other partners. and complies with the Home Office Surveillance Camera Code of Practice, issued by the Home Office which is overseen by the Surveillance Camera Commissioner and in particular the 'Guiding Principles' set out within that code; and 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Information' issued by the Information Commissioner's Office.

5.2 Future Revision and Consultation

This Policy will be subject to regular review, which will at the very least be annual.
This Policy is supported by a Standard Operating Procedure (SOP) Manual, which is a restricted document and is for the use of CCTV Staff only.

Section 6 CCTV Equipment

6.1 Cameras

The public space CCTV scheme consists of 87 permanent networked colour CCTV cameras of various designs, some of which are static, and others have a pan, tilt and zoom (PTZ) facility. These cameras are predominantly in the Town Centres across Havering. The scheme was previously merged with the 260 Housing Estate cameras. (*CCTV numbers are likely to expand in 2025-26 due to the CCTV refresh project and new housing development builds)

The images from these cameras are transmitted back to CCTV Control Room via hard wired or wireless systems.
The CCTV Control Room houses the command-and-control equipment for the cameras as well as the central digital video recorder.
CCTV Operators review a selection of the above cameras every shift.

A location map and list of the cameras will be made available on our CCTV web page.

6.2 Rapid Deployment (Mobile) Cameras and the JET group

Havering Council currently has 8 rapid deployment cameras (RDC) that can be moved from time to time to priority locations in the borough. These cameras are not monitored continuously but they do record 24/7 and can be checked retrospectively by the Control Room staff. The deployment of these cameras is bid for by partners at the monthly Joint Enforcement Tasking (JET) meetings which are attended by council officers, emergency services and other partners with a responsibility for community safety. The typical deployment for these cameras is usually three months at a given location, but each camera is assessed on a case-by-case basis at the JET meetings with some cameras being deployed for longer if required. These cameras are generally deployed to deal with ASB and Enviro-crime hotspots.

Footage obtained from any of the council's CCTV cameras may be used to seize vehicles involved in serious environmental crime and/or prosecute the owners where appropriate or to issue Fixed Penalty Notices (FPNs) to offenders. These actions can be carried out under the Environmental Protection Act 1990 and Control of Pollution Act 1979 powers.

The council makes no distinction between networked and rapid deployment cameras, and all are operated in line with this Policy.

6.3 Dummy & Covert Cameras

The council does not currently deploy dummy CCTV cameras.

6.4 Recording of Audio

Cameras forming part of the Havering Council public space CCTV scheme do not have the facility to capture and record audio.

6.5 Signage

The council has a consistent CCTV signage policy. All areas where CCTV is in use will have clear signs exhibited to comply with the Data Protection Act 2018; this is to advise people that they are in or are about to enter an area covered by CCTV cameras. The signs will also act as an additional deterrent.

Signs will carry the outline of a CCTV camera. The information on the sign will explain why the CCTV camera(s) are there, including traffic enforcement purposes, who operates them (Havering Council) and contact details including a telephone contact number as well as an email or web address directing people to the council's CCTV web page. The signs, position and the message will be large enough to enable people to easily read the information on it.
(An example of the current CCTV design can be found in Appendix 1.)

6.6 Network Maintenance

To ensure compliance with the Surveillance Camera Commissioner's (SCC) Code of Practice, especially principle 8, and to ensure that images recorded continue to be of appropriate evidential quality, Havering Council have entered into a maintenance contract to provide fault rectification and pre-planned preventative maintenance with an approved specialist provider.

Section 7 Control Room Management

7.1 Control Room Location

The control room is now on the Havering Town Hall Campus. However, it is not a public facing facility and visits to the control room other than by authorised persons are not permitted.

7.2 Control Room Standards

The Control Room is managed to meet the minimum requirements set out in the Surveillance Camera Commissioner's Guidance for in-house monitoring centres who monitor their own surveillance camera systems only, and do not have contracts to monitor third party surveillance camera systems.

7.3 Hours of Operation and Staffing of the Control Room

The Control Room is managed, monitored and controlled by Havering Council. All staff currently monitoring the cameras and operating the intelligence are directly employed by Havering Council. The Control Room is staffed 24 hours a day, 365 days a year other than by exception due to illness or mandatory staff training.

7.4 Authority for Control Room Access

The manager responsible for CCTV is authorised to decide on behalf of the Council who has access to the Control Room.
This will normally be:

- Staff employed to operate the Control Room
- Police Officers authorised in a manner agreed between the Metropolitan Police and Havering Council
- Requiring viewing recorded data of a particular incident, or
- Taking written statements from a member of the Control Room staff who viewed a specific incident being investigated or
- Collecting recorded media being considered or used for evidential purposes or other specifically agreed purpose
- Acting as liaison officers for major events or operations
- Other enforcement agencies by prior agreement
- Building, network and Control Room systems maintenance contractors by prior arrangement
- Accompanied visitors by prior arrangement with the manager responsible for CCTV or their nominee

7.5 Authority for Access by Others

Any request to visit the Control Room that fall outside of those detailed above by private companies or individuals will be dealt with by the manager responsible for CCTV or their nominee.

7.6 Normal Operation of the CCTV System

The control of the CCTV system will remain with Havering Council at all times.
Only those authorised members of staff with responsibility for using the equipment housed within the Control Room will have access to the operating controls.

7.7 Secondary Control

The Borough BECC (Borough Emergency Control Centre) may be set up in the conference room within the CCTV Control Centre. Secondary monitoring facilities are accessible for viewing by Emergency Planning staff in the event of a Borough Emergency where the BECC is opened and where CCTV is relevant to an incident. However, Control Room staff will have primacy of control of the cameras at all times.
The Control Room also has the facility to send images to the Metropolitan Police Command and Control Centre at Lambeth which may assist with Tactical scene management.

7.8 Out of Hours Contact Centre

The Council's CCTV team currently takes calls from Blue Light services and other local partners in the BID districts and private shopping malls. The CCTV control room also take emergency calls from residents trapped in lifts via the lift alarms.
The CCTV control staff also have immediate contact with stakeholders using the Town Centre radio system and the Met Police Airwave Radio systems. As the BECC is contained within the CCTV control room, staff may become involved in related communication with regards to an emergency incident, however, this is usually a very rare occurrence.

All other calls to the council go via the main switchboard separate to the CCTV Control Room.

Section 8 Operational Personnel

8.1 Security Screening

All staff employed in the Control Room are required to undergo a DBS (Disclosure and Barring Service) check due to the nature of the work undertaken. This DBS check is carried out on behalf of the manager responsible for CCTV by the human resources department of Havering Council and renewed every three years. Staff are not currently required to undergo any additional vetting.

8.2 Confidentiality

All staff employed in the management and operation of the CCTV system will observe strict confidentiality in respect of all information gained and observed during the course of undertaking the management and operation of the CCTV scheme. This shall prohibit the disclosure of any such information to any third party except as may be required by law or other lawful process which may include sharing with consent.

All staff are required to complete mandatory Data Protection and Security training as employees of LB Havering.

Any breach of this condition of employment will be dealt with by Havering Council as a serious breach of discipline or considered a possible a criminal offence.

8.3 Requirement to Give Evidence

Control Room staff are required to cooperate with the police and other enforcement agencies and provide witness statements and occasionally appear in court when requested to do so.

8.4 Initial Training

All staff will be trained before they are allowed to take up a solo position in the CCTV Control Room.

All staff training will be provided and supervised by persons qualified and experienced in all aspects of the management and operation of the CCTV system and Control Room.
All staff training will take place “in house” or by qualified third party training organisation, using training courses approved by London Borough of Havering and where appropriate the Security Industry Authority (SIA).

All permanent staff will have or undertake the BTEC Level 2 CCTV Operator Course or equivalent as a mandatory qualification. Where temporary or agency staff are employed, a basic level of competency training will be offered to ensure that basic services can be provided.

8.5 On-going Training

All staff will be provided with regular ‘refresher’ training to ensure that the highest operating and management standards are maintained. Training records will be maintained for each member of staff employed in the Control Room.

Section 9 Use of the System

The purpose of the CCTV cameras is to provide surveillance of public areas only. All camera locations have clearly visible signage that will give a clear warning that CCTV is in use.
Cameras will be sited and configured to view public areas only and not overlook private dwellings or other areas where privacy is expected. However, it is not always possible to achieve this, and certain cameras may have the capacity of viewing private/unwanted locations e.g. through the zoom facility. These cameras have privacy zones installed to prevent any unnecessary infringement of privacy.
Control Room staff will only use the cameras to view public space areas and will not use the cameras to look into the interior of any premises or any other area. This clause also includes anything that may be deemed as the inappropriate invasion of personal privacy even though the person concerned may be in a public area. Any such breach of this condition will be dealt with as a serious disciplinary matter and may lead to dismissal.

9.1 Regulation of Investigatory Powers Act 2018 & Directed Surveillance

On rare occasions the CCTV cameras may be used in covert directed surveillance, as defined by the Regulation of Investigatory Powers Act 2018 (RIPA) by judicially authorised law enforcement agents. In those cases, the CCTV Control Room staff will assist them in undertaking covert directed surveillance.

Before this occurs, approval should be sought from the Senior Responsible Officer, Head of Service or Service Manager

Operators of the council’s CCTV System are trained and fully aware of RIPA issues associated with using CCTV and that continued, prolonged systematic surveillance of an individual may require an authorisation.

The use of RIPA will be undertaken in line with Havering Council’s RIPA Policy (Currently under review).

Havering Council reserves the right to refuse the use of its public space CCTV system for covert surveillance if it considers that to do so would be counter to council polices, OSC Guidance or it is reasonably believed that it is likely to result in an unwarranted breach of an individual’s right to privacy and/or where the perceived risk is unacceptable.

Section 10 Data Recording

10.1 Ownership of Copyright

All data captured by the CCTV cameras and related equipment and stored on any form of recording media held either internally or externally will remain the property of Havering Council.

10.2 Recording Retention Period of Personal Data

Recorded data will be stored for a maximum period of 31 days. The Video Management System (VMS) automatically deletes footage every 31 days and continuously overwrites data unless stored for investigation or individual rights requests. In the event incidents are brought to our attention, in particular for investigation or prosecution purposes then personal data may be held on for a longer period.

10.3 Security of Recorded Data

All images from the CCTV system will be recorded onto encrypted hard drives forming part of the Video Management System (VMS) installed within the system.
The recorded data will only be used by Havering Council, police or other enforcement agencies for the following authorised purposes:

- Investigation or identification of Person(s) suspected of criminal or anti-social behaviour;
- Production in court of law by Police or other law enforcement agency for evidential purposes;
- Use by the Council to support the undertaking of the Councils statutory duties;
- For training and promotional purposes

Under no circumstances will the recorded data be issued, given, shared with, or sold to any third parties by the Council without the approval

Section 11 Use of Recorded Data for Enforcement Purposes

11.1 Reason to View Recorded Data

When the police or other enforcement agency believes that footage of an incident has been recorded, they may request access to view the specified incident on the appropriate recording. A police officer, police community support officer or other authorised law enforcement agent will be permitted to view the recording at the Control Room on a workstation provided for this purpose and will be under the supervision of Control Room staff.

11.2 Release of Data to Police or Other Enforcement Agency

At no time shall the images supplied to the police or other law enforcement agency be used for anything other than the purpose specified and identified when the images were released from the CCTV Control Room.
The responsibility for the images safekeeping and integrity will transfer to the police or other law enforcement agency once the media has left the CCTV Control Room. The council will not be liable for any mishandling, compromise in security or other misuse of the recording media whilst in the custody of the police or other law enforcement agency.

Section 12 Use of Visual Data

12.1 Continuity of Evidence

Any images released from the CCTV Control Room to the police or other law enforcement agency will be dealt with under their existing property and exhibit handling procedures before leaving the CCTV Control Room.

12.2 Copies of Original Recorded Data

The council will not routinely store copies of recorded data. For cases outside of those used evidentially, only in exceptional cases of serious incidents or those of substantial magnitude data be retained otherwise. (e.g staff misconduct)

12.3 Handling of Recorded Data after use in Court

At the conclusion of the need to retain any original recording the police or other enforcement agency will store the recording in accordance with their procedures. Recordings will not be returned to Havering Council for storage. The police or other enforcement agency will become responsible for the destruction of the recorded data once there is no further use for it.

12.4 Request to View Recorded Data by Non-Enforcement Agencies

The procedures for handling and logging the recorded data are as described for the police or other enforcement agency, however commercial agents such as insurance companies or private law firms may be charged a fee to cover administration costs where requests for data to support civil claims or accidents are made.

Any requests from members of the general public or a third party will be dealt with under the provisions of the Data Protection Act 2018 or the Freedom of Information Act 2000.

12.5 Release of Images for Entertainment Purposes

The Council will not release any images, either directly or indirectly, to any organisation for inclusion in any television or other media production designed purely for entertainment purposes or educational/factual programs. Likewise, material can only be released to the media as part of an ongoing crime investigation by Police with the permission of the Head of Enforcement & Community Safety.

Section 13 Data Protection

13.1 Introduction

The Council takes the security and privacy of data seriously and is committed to being transparent about how we collect and use personal data and meet our data protection obligations.

13.1.1 Data Controller

We are registered as a “data controller” with the Information Commissioner’s Office (ICO) and will comply with our legal obligations under the Data Protection Act 2018 (the “2018 Act”) and the UK General Data Protection Regulation (“GDPR”).

13.2 Data Protection Officer

The Council has appointed an Information Governance Manager who is the Data Protection Officer (DPO). Their role is to inform and advise the council of its obligations under data

protection legislation and to monitor the council's compliance. The Data Protection Officer also acts as the single point of contact for the Information Commissioner's Office (ICO) and provides advice and assistance on Data Protection Impact Assessments (DPIA).

The DPO can be contacted at DPO@Havering.gov.uk. Further information is available on the council's website.

13.3 Data Protection Definitions

There are two types of data under the Data Protection Act 2018:

- Personal Data – any information relating to an individual who can be identified from that information (Data Subject) on its own or when taken with other information. This may include facts and expressions of opinion about the subject and indications of the council or others in respect of the subject. It does not include anonymised data.

- Special Category Data – which means processing information about a person's racial, ethnic origin, political opinions, religious beliefs, trade Union membership, health data, sex or sexual orientation as well as genetic and biometric data.

Images collected by the Havering Council public space CCTV scheme will normally fall under the "Personal data" category.

13.4 Lawfulness of processing

The Council uses CCTV cameras as a proportionate response to support the Community Safety Strategy of the Council and work with its partners to reduce both the level and fear of crime. It achieves this in several areas including:

Assisting the police and other law enforcement agencies in the apprehension and prosecution of those committing crime and public disorder;

- Evidence gathering by a fair and accountable method
- Providing a visible deterrent to crime, thereby providing reassurance to residents and business alike;
- Assisting in aspects of town centre management and traffic enforcement;
- Improving the safety and security of residents, visitors and the business community who use the facilities in the areas covered.
- Assisting with the location of missing persons notified to the Control Room by police. This will be carried out under the UK General Data Protection Regulation under Article 6 (d) "vital interests" which is described as the processing of information necessary to protect someone's life.

The lawful basis used to process CCTV images as set out in the UK data protection legislation are:

- UK GDPR Article 6(1)(c) Legal obligation: the processing is necessary for us to comply with the law
- Uk GDPR Article 6(1)(e) Public task: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law
- UK GDPR Article 6(1)(f) Legitimate Interests: the processing is necessary for our own legitimate interests

Where we process special category data, the lawful basis is:

- UK GDPR Article 9(2)(g): processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

The relevant basis in UK law is set out in section 10(3) of the DPA 2018. This means that we're required to meet one of the 23 specific substantial public interest conditions set out in Schedule 1. The substantial public interest condition is one or more of the following:

- Sch 1 para 7: Administration of justice
- Sch 1 para 10: Preventing or detecting unlawful acts
- Sch 1 para 11: Protecting the public
- Sch 1 para 20: Insurance

Where personal data relating to criminal allegations or offences is processed, this will be carried out only where authorised under UK law in compliance with UK GDPR Article 10 and will meet one or more of the following conditions set out Schedule 1, Part 3 of the Data Protection Act 2018:

- Sch 1 para 33: Legal Claims
- Sch 1 para 36: Substantial Public Interest
- Sch 1 para 37: Insurance Claims

13.5 Data Subject Access Requests

Individuals have the right to request a copy of their personal data being processed by the council. In the case of CCTV footage this will always be in electronic form.
Havering Council will not permit viewings or release images to people being investigated by an enforcement agency including the police where images have been handed over as part of the investigation. The responsibility for investigating and disclosing images to those involved in the investigation are covered by the Police and Criminal Evidence Act 1984 (PACE) and the Crown Prosecution Service (CPS) Evidence and Disclosure Policy which prosecuting authorities are required to follow. It should be noted that other enforcement agencies will operate under other legislation but the use of and disclosure of evidence rests with them.
The council will respond within one month unless the request is complex or numerous in which case the period can be extended by a further two months. If an extension is necessary, the council will write to the individual within one month of receiving the original request to explain why an extension may be necessary.
If a subject access request is manifestly unfounded or excessive the council is not obliged to comply with it. Alternatively, the council may charge a fee based on the administrative cost of responding to the request.
The council will explain to an individual if they refuse to respond to a request and of their right to complain to the Information Commissioner's Office.
Requests for CCTV footage can be made by using the forms that can be found on the council's CCTV website.
The Council may need to ask for identification before the request can be processed.

13.6 Data Security

The council takes the security of personal data seriously. The council has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure and to ensure that data is not accessed, except by those who have lawful authority in connection with the proper performance of their duties.

The council recognises that the personal data it holds is valuable and must be managed properly as accidental loss, unlawful destruction or damage may cause distress to individuals concerned.
Examples of our security of CCTV footage include:

- Encryption - meaning that information is hidden so that it cannot be read without special knowledge (such as a password). This is done with a secret code or what is called a “cypher”. The hidden information is said to then be “encrypted”.
- Controlling access to systems and networks allows us to stop people who are not allowed to view personal information from getting access to it.
- Regular testing of technology and upgrading security measures including keeping up to date on the latest security updates (commonly called “patches”).
- Training of staff to make them aware of how to handle personal information and how and when to report when something goes wrong.

13.7 Staff Training and Guidance

Everyone who works for or on behalf of the council has responsibility for ensuring data is collected, stored and processed appropriately in line with the Data Protection Act 2018 and relevant policy.
The council has in place a Data Protection Policy which explains the obligations of employees, workers, consultants, volunteers, interns and apprentices when obtaining, processing or storing personal data in the course of working for or on behalf of the council.

13.8 Further Information

If you require any further assistance the council’s website https://www.Havering.gov.uk contains a range of information regarding information management. A link to the Councils Privacy Notice can be found here CCTV Privacy Notice

Section 14 CCTV System Review

14.1 Operational Requirements

Operational requirements are used by the council to thoroughly assess the necessity of CCTV cameras and systems to ensure full consideration has been made of all implications relating to their installation. An Operational Requirement is “A statement of needs based on a thorough and systematic assessment of the problems to be solved and the hoped for solutions.” Pertinent questions are:

- What is the problem?
- Will CCTV help solve the problem?
- What other solutions have been considered? Can we afford what we want?
- Is what we do compatible with existing infrastructure and technology? The period of retention of data/images;
- The frame rate suitable to achieve minimum evidential quality and the compression method.

Only once the above questions have been satisfactorily answered will the council install additional CCTV cameras.
Any additional cameras will be installed in compliance of the ‘Surveillance Camera Code of Practice Pursuant to Section 29 of the Protection of Freedoms Act 2012’.

14.2 Privacy Impact Assessments

All Public Realm and Housing camera deployments will be covered by Privacy Impact Assessments (PIA). A PIA is a separate process from compliance checking and will be completed when a new CCTV system is being considered, or an existing system is modified (i.e. if re-deployable units are moved)

Section 15 Legal Requirements

15.1 CCTV Staff Legal Requirements

At all times, and without exception, Havering Council's CCTV Control Room and its staff will comply with all legislation, directives, policies, codes of practice and guidelines relating to the operation of the CCTV System.

All officers, supervisors and staff of Havering Council's CCTV system are trained in all their responsibilities to meet the requirements under the above paragraph, with a planned ongoing review programme in place.

15.2 Applicable Legislation

In addition to council policies, procedures, guidelines and codes of practice, operational procedural manuals, CCTV and its operation are subject to legislation under:

- The Data Protection Act 2018 –& UK GDPR ensuring that all personal data is protected and private
- A Data Protection Code of Practice for Surveillance cameras and Personal Information
- The Human Rights Act 1998 – Article 8 gives individuals the right to privacy, Article 6 gives individuals a right to a fair trial and Article 5 gives the right to Liberty and Security.
- The Regulation of Investigatory Powers Act 2018 – applying to directed surveillance from our overt CCTV systems
- The Freedom of Information Act 2000 – all applies to all recorded data held by the Council apart from Environmental Information that is covered by the Environmental Information Regulations 2004 and personal data that is covered by The Data Protection Act 2018
- The Private Security Industry Act 2001– where required by the Act, operators of CCTV will be licensed under the Act
- Section 17 of the Crime and Disorder Act 1998, which requires the key partners to the strategy to integrate crime reduction within their mainstream activities
- The Protection of Freedoms act 2012 which sets out the criteria where PSS cameras justify a 'Pressing Need'
- Surveillance Camera Code of Practice

Section 16 Complaints Procedures and Comments

16.1 The Procedure for Complaints against the CCTV System

Any complaint received regarding CCTV operations will be dealt with by following the complaints procedure laid down by London Borough of Havering.

Information on how to complain is contained on Havering Council's website

16.2 Comments Regarding the CCTV System

Anyone wishing to make comments or observations about the CCTV system should write or email the manager responsible for CCTV CCTV@Havering.gov.uk

16.2.1 Complaints about private CCTV

Private CCTV systems are not covered by this CCTV Policy. However, all private CCTV systems should also be operated with the same principles as the above.

Advice on what to do if you have concerns about a private CCTV system can be found on the ICO Website at the following location Home CCTV systems | ICO

If you are a Council tenant or Leaseholder living in a Havering Council owned property you must seek permission from the Housing Department before installing any CCTV equipment. Failure to do so may result in the Council taking legal action requiring you to remove the equipment.

Section 17 Provision of Public Information

17.1 Annual Report

Factual information on the numbers of the cameras, their location and statistical findings of their effectiveness will form part of the evaluation process and may be published to a limited extent periodically and/or subject to regular scrutiny by the relevant Overview and Scrutiny Committee.

Part 3 Body Worn Video

Section 18

18.1 General

The Information Commissioner's Office considers BWV systems as being likely to be more intrusive than conventional CCTV. As such, any use of BWV should be proportionate, necessary and meet a pressing social need. Accordingly, the Council has established four aims for the use of BWV, ensuring the organisation's broad use of BWV is compatible with this requirement. These are:

- Improve Staff Safety: Utilising BWV to improve staff safety by capturing objective evidence of threats or assaults, strengthening the ability of the Council and the police to prosecute those responsible. Additionally, the visible presence of BWV can serve to discourage threats or assaults as perpetrators are aware that they are at greater risk of being identified.

- Reduce Complaints: By capturing objective evidence of interactions between staff and individuals, false or frivolous accusations are reduced, while providing useful evidence to resolve legitimate complaints.

- Improve Enforcement: BWV provides a valuable tool that staff can use to document incidents and capture evidence, providing an additional, powerful tool to assist investigation and enforcement activity.

• Support Problem Solving: BWV provides a practical tool for staff to gather information that can easily be shared. By using BWV to gather information that may not otherwise be recorded, the effectiveness and efficiency of the Council's enforcement services as a whole can be maximised.

Unless being used for a specific evidential or problem-solving purpose, the camera must be positioned to capture a clear view of interactions between the officer and the public. When in use, the camera must be positioned in such a manner that it is visible to an individual being recorded by that camera (for example, it should be worn on top of the officer's outer layer of clothing).

Each officer must sign out and return their assigned camera at the beginning and end of each shift. This ensures accurate records are maintained of which member of staff used which device, allowing footage to be correctly attributed. When returning the camera at the end of their shift, the member of staff must re-dock it to enable the video to be uploaded and battery recharged.

BWV equipment used by officers should be set up so that live video images are not displayed on the camera while it is in use. This will ensure that potential confrontations are not escalated by an individual's knowledge that an officer has activated their camera during an exchange. Staff must provide a clear warning to inform individuals they are being recorded.

All staff must receive appropriate training and a full briefing on the use of BWV prior to or at the time of issue. This ensures they are fully equipped to operate the equipment safely and in accordance with this policy.

Staff using BWV must provide details of how an individual can obtain a copy of any video footage captured.

18.2 Using Cameras

The situations where staff are expected to make use of BWV will vary, and their judgement will be required to determine whether they need to make use of BWV equipment, in line with the BWV aims.

Improving Staff Safety: BWV cameras should be activated in situations where the staff feel unsafe, or where they believe that there is a risk of physical injury or harm or verbal assault to themselves, other officers or members of the public. Additionally, if a member of staff is subject to an assault, or witnesses such an assault, they must activate their camera as part of evidence gathering process.

Reducing Complaints: While the majority of interactions between members of staff and the public are peaceful and do not result in complaints, there is a risk that some individuals will not perceive their experience to be a positive one. BWV cameras provide an opportunity to capture an objective record of an interaction, providing clear evidence of the behaviour of the individuals involved. As such, staff should activate their BWV camera (after giving a clear verbal warning they are doing so) if they identify a situation as being one where a potential confrontation could occur and that a recording would be beneficial to both parties in providing a record. Particular consideration should be given to situations where enforcement action is taking place with the individual present (for example, issuing a PCN when the driver is present), and may seek to challenge the conduct of the CEO carrying out that enforcement.

Improving Enforcement: BWV cameras support the gathering of video evidence in real time when undertaking enforcement activities or associated inspection work. Staff should therefore activate their cameras in situations where the evidence gathered through the recording will be

evidentially beneficial to the conducting of investigations or enforcement, such as to provide evidence of a particular situation or to facilitate the subsequent identification of individuals. Discretion must be shown to avoid unnecessary or excessive intrusions into the privacy of individuals, particularly third parties, beyond that required to document a potential incident, while balancing the other enforcement aims.

Supporting Problem Solving: As part of the broader approach to problem solving and integrated enforcement, services may request that other enforcement services look out for particular issues or information when carrying out their duties that they would not otherwise report. In these situations, recording this information on BWV provides an opportunity to gather and share this information quickly and effectively, without requiring an extensive time commitment from staff focused on their core duties.

All use of BWV equipment must be in line with at least one of the Council's four BWV aims. Inappropriate use of BWV equipment, particularly in situations where recording is excessive and causes unnecessary intrusion (for example, in breach of the Voyeurism (Offences) Act 2019) may be subject to disciplinary action.

18.3 Authorised Officers

Authorised officers are typically managers or supervisors, who will have responsibility for reviewing recorded BWV footage as required, as well as for editing and sharing footage in line with the BWV aims.

Authorised officers are required to confirm that they are aware of the potential sensitivity of the data that they are accessing, that they are aware of the Council's responsibilities under the General Data Protection Regulations (GDPR), Data Protection Act 2018 (DPA2018), as well as the need to ensure that BWV recordings are used appropriately and in line with the BWV aims.

18.4 Viewing and Editing Recordings

Just as the use of BWV equipment must align with at least one of the Council's four BWV aims, the processing and use of recordings must also align with at least one of these four aims, and be proportionate, necessary and meet a pressing social need.

BWV equipment will be configured by default not to allow video to be played back on the device itself, with authorisation to allow device playback requiring the agreement of an authorised officer or the relevant senior manager. While it is acknowledged that instant playback may be beneficial to officers in some situations, restriction of this feature limits the ability for misuse, as an authorised officer is required to provide playback access.

The ability to delete or edit recordings within the device will be restricted. This is to ensure confidence in the recordings, by providing assurance that officers who may be involved in an altercation are not able to modify recordings themselves. Additionally, by restricting the ability to edit recordings to authorised officers, it ensures that any changes (such as concealing third parties' identities), is carried out in line with evidential and legal requirements.

Recordings not identified by BWV equipped officers or authorised officers as evidential or otherwise required will be automatically deleted after 90 calendar days from the date of the recording.

Authorised officers may only access recordings for which they have been granted prior approval. Access must be controlled and auditable. By default, authorised officers have

permission to view recordings associated with their own service areas, and may view recordings shared with them by other authorised officers.

When viewing (or sharing recordings as below), authorised officers and their managers must be mindful of any footage which is or could be considered traumatic in nature. Appropriate precautions should be considered to reduce any risk of that officer or indeed another being adversely affected (e.g. vicarious trauma). Senior managers should be advised of any such footage as soon as practicable and ensure appropriate measures are put in place to ensure staff are supported and any such risks are minimised. This could include provision of warnings before viewing/sharing, viewing at certain times/locations, or prohibiting viewing.

18.5 Sharing Recordings

The sharing of recordings between authorised officers must be carried out for purposes relating to at least one the four aims, such as to share evidence gathered to support problem solving or to support an investigation, or to assist in the identification of an individual suspected of any criminality.

External partners and Council services that do not utilise BWV equipment must not be given direct access to the BWV system without the agreement of the relevant senior manager. The sharing of images outside of the BWV system must be carried out through an agreed secure method in accordance with the Council's data protection protocols. If future technological advances allow, the council will seek to limit the sharing of images via a secure portal / file sharing system.

Authorised officers are responsible for ensuring that any redactions required prior to sharing (such as anonymising third parties) are carried out. The audio and visual elements of recordings may have different levels of sensitivity depending on content, and consideration therefore needs to be given to the contents of both elements when sharing.

All physical media used to store BWV images must be appropriately encrypted, in line with data protection protocols and best practice.

Authorised officers must be mindful that the sharing of personal information relating to living individuals is subject to the provision of the GDPR, DPA2018 and associated legislation, and must ensure that the appropriate legal processes have been completed to enable this information to be shared, such as via Schedule 2 request or Data Sharing Agreement.

18.6 Individual Rights

Under the GDPR and DPA2018, individuals have a range of rights in respect of their personal data, which can include audio-visual recordings. Of these rights, it is anticipated that individuals are likely to seek to use two rights in respect of BWV recorded sound and images: the Right of Access (also known as Subject Access Request) and the Right to Erasure.

Under the Right of Access, individuals can request copies of information that the Council holds about them, including audio-visual recordings. This presents potential challenges for authorised officers, who will need to identify the individual and determine whether the Council holds recorded images or sound relating to them. It is therefore advisable to start the process with the request itself, as the individual may be requesting footage of a specific interaction, or with any enforcement action relating to that individual, which may have been recorded. As part of the Right of Access process, individuals are required to provide photo-ID, which can be crosschecked against the recording. Third parties' images and personal data must be redacted.

Under the Right to Erasure, individuals can request that information that the Council holds about them be deleted, and that information that cannot be deleted is subject to restrictions on how it can be used. As with the Right of Access, the individual in question would need to be identified, and relevant footage reviewed to determine if the individual has been recorded. The context in which the individual has been recorded is important, as it will inform whether the Council has to comply with the request. When deleting information, the authorised officer will need to take a view on the extent to which deletion or anonymisation (such as blurring the individual) is more appropriate, depending on the content and purpose of the recording and the nature of the recording of the individual.

There is a range of exemptions that apply to both Right of Access and Right of Erasure in the context of law enforcement activity. In the event of a request to exercise either right in respect of BWV, authorised officers should liaise with the Information Governance/GDPR service.

For information on how you can obtain a copy of video footage taken by a body worn camera or the Data Protection rules, which govern the use of a body worn camera, please visit our website: and request the footage.

Signatories:
Signed: ____C McAvoy_____

Chris McAvoy
For and on behalf of London Borough of Havering
Title: Head of Enforcement and Community Safety, Place
Date: 01/03/2025

Appendix A – Example of current CCTV signage

CCTV Policy EQIA 2025.docx