

London Borough of Camden

CCTV Code of Practice v0.03 24/03/2023 09:59:00



KEY CCTV/AUTHORISED OFFICERS AND THEIR RESPONSIBILITIES:

Job Title	Officer Responsibly (This list is not exhaustive)
CCTV Corporate Owner	Head of Property and Security Services
CCTV SPOC	Reports to CCTV Corporate Owner and Head of Security.
Authorised Officers/Responsible Officers (who process CCTV)	One Officer nominated in each service where applicable
CCTV Operators (contracted out)	Who also have regard to this, Camden Code of Practice and the Home Office Code of Practice

Contents

1. Introduction
2. Objectives of the CCTV systems including Body Worn Video (BWV)
3. Principles
4. Ownership and Management of CCTV systems
5. Management and Operation of CCTV systems
6. Installation and Privacy
7. Assessment of CCTV systems and Code of Practice
8. Maintenance of CCTV equipment
9. Management and Operation of CCTV systems and Recorded data
10. Surveillance Code of Practice
11. Protection of the Freedoms Act 2012
12. Data Protection Act 1998 (DPA) and Regulation of Investigatory Powers Act 2000 (RIPA)
13. Information Commissioners Office (ICO) In The Picture
14. Subject Access Request (SAR) Request for Personal Data
15. Public Information
16. Security, Complaints and Breaches of Code

1. Introduction

- 1.1** Camden Council own, operate and manage the data of closed circuit television (CCTV) systems that survey public areas, council buildings and housing estates throughout the borough.
- 1.2** Public Space (highway) CCTV cameras located around the borough on the highway. These cameras are monitored 24/7/365 in real time recording. Recordings are retained for 31 days and thereafter automatic erasure unless saved to hard drive. Saved data is retained for one calendar year. There are many other CCTV within the borough of Camden owned and operated by private members of the public, the Police, businesses and Transport for London (TfL).
- 1.3** Housing CCTV located around many of the council own land. Most of these cameras are monitored 24/7/365 in real time recording. There are some sites where recording is done locally – on site. Recordings are retained for 31 days and thereafter automatic erasure unless saved to hard drive. Saved data is retained for one calendar year.
- 1.4** Corporate CCTV located around the council's corporate buildings which include the council own libraries. Some of these cameras are monitored 24/7/365 in real time recording. There are some sites where recording is done locally – on site. Recordings are retained for 31 days and thereafter automatic erasure unless saved to hard drive. Saved data is retained for one calendar year.
- 1.5** Body Worn Video is used by the council's contracted Responsive Security Patrol Officers (RSP) who patrol the council's housing land. These cameras record at the sole discretion of the RSP officer. Once activated the camera records visual images and audio in real time until the RSP office stops the recording. Recordings are retained for 31 days and thereafter automatic erasure unless saved to hard drive. Saved data is retained for one calendar year.
- 1.6** Our control room facilitates the use of a police radio. Local police have access to live, post images from the cameras so we can quickly notify them if there is an incident. Recordings retained for 31 days and thereafter automatic erasure unless saved to hard drive. Saved data retained for one calendar year.
- 1.7** All Public Space Camden owned CCTV have signage stating purpose and contact details. Work is underway to roll out signage across the council housing estate and corporate CCTV portfolio whilst carrying out upgrade works.
- 1.8** This Code of Practice applies to all CCTV systems owned or operated on behalf of Camden Council, in public, housing land and corporate site areas.
- 1.9** The designed CCTV Code of Practice is to ensure the Council's CCTV systems be managed effectively, efficiently and lawfully. A live Service Operating Procedures (SOP) supplements this code, on how individual systems are, operated in accordance with the code.
- 1.10** Camden operates CCTV in partnership with the Metropolitan Police, TFL and other stakeholders.

1.11 The same principles and governance apply to the deployment of Body Worn Video (BWV) as with CCTV cameras and is included within the Council's CCTV policy.

1.12 Body Worn Video (BWV) is also operational within the borough. Some Security and Patrolling Council and contracted officers issued with a BWV as part of their uniformed daily routine. Officers will activate their BWV in the event of threat, safeguarding or evidence gathering relating to persons and or property.

2. Objectives of the CCTV systems

2.2 The objectives of the CCTV systems are:

- To reduce the fear of crime promoting a feeling of safety.
- To deter crime, detect crime and provide evidence of offences
- To deter and assist in anti-social behaviour.
- To identify and or monitor risk and vulnerability.
- To assist in providing the safety and security of employees, members of the public, building and assets.
- To enhance community safety, assisting in developing the economic well-being of Camden and encourage greater use of the borough's public open spaces, facilities and amenities.
- To detect and prevent environmental issues
- To assist the Local Authority in its enforcement and regulatory functions.
- To assist in highways management.
- For the provision, for enforcement of parking and moving traffic regulations to promote compliance and is carried out in part through CCTV.
- To support civil proceedings.
- To support the Council's integrated transport policy.
- To assist the Council in delivering its statutory and other functions.
- To assist in the management of Council premises.
- To assist the Council in its overall resilience planning linked to civil contingency planning, emergency response and business continuity functions.

3. Principles

3.1 Individual CCTV systems operated fairly, lawfully and in accordance with this code.

3.2 Each CCTV system operated to ensure the privacy of the individual and their human rights. The Human Rights Act 1998 gives effect to the rights set out in the European Convention on human rights. Some of these rights are absolute, whilst others are qualified, where it is permissible for the state to interfere so long as it is in pursuit of a legitimate aim and proportionate.

3.3 Application of this code will ensure that CCTV systems are installed and operated in such a manner as to preserve the right to respect for private and family life conferred by article eight (8) of the European Convention on Human Rights. Adherence to the code will ensure correct handling of recorded images, which will avoid breaches of article six (6), the right to a fair

hearing. The public interest in the operation of CCTV systems maintained through the security and integrity of Service Operational Procedures manual (SOP).

4. Ownership and Management of CCTV systems

- 4.1** . Camden Council own, manage and are responsible for the compliance with this code, ensuring the rights and interests of the public and of individuals are maintained.
- 4.2** The day-to-day operation of the systems is the responsibility of the Council and or its providers contracted by the Council for such purpose. In compliance with the Information Commissioners Office (ICO) CCTV Code of Practice – In the Picture. All systems should be properly signed to inform members of the public who to contact about the management and purposes of the system.

5. Management and Operation of CCTV systems

- 5.1** Only authorised, Security Industry Authority licenced (SIA), Non-Police Personnel Vetting Level 1 (NPPV1) and Disclosure Barring Service (DBS) and signed off trained persons are to operate CCTV systems and associated equipment. Refresher annual training for operators and supervisors with applicable re-applications for SIA Licence, Police Vetting and DBS checks.
- 5.2** The operators of the system will be required to adhere to this code of practice at all times. The Council and the Council contracted staff will be subject to their employer’s disciplinary procedures in the event of a breach of this code and/or Service Operational Procedures (SOP).
- 5.3** Camera and associated equipment usage shall concur with the purposes and key objectives of the CCTV scheme and shall comply with this code.
- 5.4** Only Council members of staff or contracted staff with responsibility for using the equipment shall have access to operating controls. Operators of the CCTV system must act with the utmost integrity and take personal responsibility.
- 5.5** A requirement of confidentiality will be enforced during and after termination of employment. A CCTV confidentiality form must be signed and annual renewal for individuals deployed within the CCTV Control Room.
- 5.6** CCTV systems are to be audited annually to ensure the requirements and objectives to operate the system still remains. This applies also to the requirement of collecting and retaining personal data ensuring other legal requirements, policies and standards are complied with in practice. This is in accordance with the Information Commissioner’s (ICO) CCTV code of practice (2014), the Secretary of State’s surveillance camera Code of Practice (2013).
- 5.7** Security of the CCTV control room and recorded material CCTV monitoring and control equipment and access to recorded images is to be restricted and only used for the purposes stated in or referred to in this code.
- 5.8** Recorded images are to be kept securely at all times and live and recorded images are only to be viewed and reviewed to meet the purposes of each system. Access to the Council’s CCTV

equipment and control room(s) is to be restricted to those managing, operating or maintaining the CCTV Control Room and its systems.

- 5.9** A log is to be maintained of all visitors to the control room(s) recording the visitors' confirmation that they will maintain the confidentiality of control room operation along with personal data and the time of arrival and departure. Visitors are NOT permitted to use the systems.
- 5.10** Members of the broadcast and print media will not be permitted access to the control rooms and CCTV equipment unless authorised in writing by the Council's data protection senior information risk owner (SIRO).
- 5.11** The system operators will hold prime responsibility for ensuring there is no breach of security and that this code is complied with at all times. They will have day-to-day responsibility for the management of the control room and for enforcing the disciplinary code.
- 5.12** The systems operator will ensure that any serious breach of this code is duly notified in accordance with the Council's Data Protection Act policies and procedures. Staff will perform their duties ensuring strict compliance with this code, agreed operational procedures and with due regard to confidentiality.
- 5.13** Any breaches will be subject to investigation and possible disciplinary action in accordance with the Council or its contractor's procedures.
- 5.14** Police use of the CCTV systems applies equally to the police and other statutory investigation agencies use of the CCTV systems.
- 5.15** Where a police operation requires a RIPA authority, the authorisation for such surveillance must be produced before the CCTV equipment is used and the authorisations must be retained securely. A 48hrs window of pending authorisation is in place allowing for weekends/bank holidays where authorising Council Officers may be limited.
- 5.16** Access to the control room will be permitted to duly authorised Police Officer(s) for the purposes of taking written statements and use of the CCTV equipment including partnership working.
- 5.17** Police use of the CCTV system, including both the review of recorded as well as viewing live images, is to be strictly controlled including logging.
- 5.18** No police officer or member of police staff is to use the CCTV equipment without permission and unless there is a clear operational requirement to do so.
- 5.19** Details of each and every use is to be recorded on the applicable police URN log or in a book kept for the purpose, both at the time of release and recovery of the system.

5.20 Any remote control and recording of cameras will strictly adhere to this code of practice and special management and data protection Team arrangements placed.

6. Installation and Privacy

6.1 All CCTV images must be adequate for the purpose for which they are collected and surveillance cameras should be sited in such a way that they only survey those areas that are intended to be viewed by the equipment. Where privacy intrusion is heavily identified steps must be taken to remove/minimise intrusion.

6.2 Permanent and or relocatable cameras should be sited and images captured restricted to ensure that they do not view areas that are not of interest and are not intended to be the subject of surveillance, such as individuals' private property.

6.3 The cameras must be sited and the system must have the necessary technical specification to ensure that images are of a suitable quality for the purpose for which the system was installed.

6.4 Prior to installation of a new system or addition to an existing system, the Council is to consult with stakeholders and the community.

6.5 The assessment for installation should aim to establish clear Operational Requirements (OR) for the camera(s) and or systems and take into account the benefits gained.

6.6 The assessment for installation should also demonstrate whether or not other or better solutions exist and what effect it may have on individuals and their privacy.

6.7 The Council will consider whether it is justifiable in the circumstances and a proportionate response to the issue being addressed. From time to time re-locatable or transportable cameras may be installed **temporarily**. The use of such cameras and the data produced by their use will always accord with the objectives of CCTV and this code.

6.8 Installation meet the requirements of the [Home Office Scientific Development Branch CCTV Requirements Manual 2009](#)

6.9 Some people regard surveillance cameras as an infringement of personal liberty. Everyone has the right to respect for his or her private and family life in line with [Data Protection Act 1998](#). Where there is an expectation of privacy, the cameras have masking applied. CCTV operators trained on how best to manage operating cameras eliminating or reducing intrusion of privacy.

7. Assessment of CCTV systems and Code of Practice

7.1 The Council will ensure the CCTV systems and this Code of Practice are evaluated at regular intervals to assess crime, anti-social behaviour, security and safety impact on neighbouring areas without CCTV, the views of the public and the operation of this code.

7.2 The Council officer with the day-to-day responsibility for CCTV (CCTV Single Point of Contact – SPOC) will continuously monitor the operation of the CCTV system and the implementation of this code.

8. Maintenance of CCTV equipment

8.1 CCTV systems and associated equipment are to be repaired, maintained and kept in full working order so as to meet the Operational Requirements.

9. Management and Operation of CCTV systems and Recorded data

9.1 Management of recorded data/material, including still image prints, will only be used for the purposes defined in this code and access restricted.

9.2 Recorded material will under no circumstances be sold or used for commercial purposes or for the provision of entertainment.

9.3 The Council may use recorded images for training purposes and to promote the effectiveness of its CCTV systems.

9.4 No more images and information should be stored other than that which is stringently required for the stated purpose of a surveillance camera system.

9.5 Such images and information should be deleted once their purposes have been discharged. This is typically 31 days, though this may vary from scheme to scheme. Retained data is held for one calendar year and should be then deleted.

9.6 Showing the recorded images to members of the public will only be permissible in accordance with the law, either in compliance with the prerequisites of the police in connection with investigation of crime, or any other circumstances provided by the law. Access to recorded images by the police, other statutory investigation agencies or officers of the court is permissible under the [Data Protection Act 1998](#), [Police and Criminal Evidence Act \(PACE\) 1984](#) and the [Criminal Procedures and Investigations Act 1996](#).

10. Surveillance Code of Practice

10.1 12 Guiding principles from the [Surveillance Camera Code of Practice](#) issued by the Secretary of State in June 2013:

1. Use of a surveillance camera system must always be for a specified purpose in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The use of a surveillance camera system must take into account 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 of access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance 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 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 systems images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10. There must be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports 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 of evidential use.
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.

11. Protection of the Freedoms Act 2012

11.1 The CCTV Control Room is strictly controlled and with risks managed at all times to ensure compliance with the Data Protection Act and UK GDPR is not breached. Data Protection Act and UK GDPR. London Borough of Camden is the Data Controller for all surveillance in the CCTV Control Room and systems. The data and information transmitted and recorded in the CCTV Control Room is confidential, classified and sometimes sensitive. Access to Data security and ethical considerations are paramount to Camden Council. Our CCTV policy complies with relevant

guidance and law, including the Human Rights Act, the Equality Act, the Data Protection Act and UK GDPR, and the Data Ethics Framework.

11.2 [Protection of Freedoms Act 2012](#) and the [Surveillance Camera Code of Practice](#) issued by the Secretary of State under S.30 of the act:

- Established a framework for CCTV surveillance, CCTV systems and associated equipment, provides a balance between public protection and individual privacy.

The Council and the police must regard the surveillance camera code of practice and abide by the 12 guiding principles in Section 2.6 which are set out in Annex 1.

12. Data Protection Act 1998 (DPA) and Regulation of Investigatory Powers Act 2000

12.1 [Data Protection Act 1998](#) (DPA 1998), and the [Regulation of Investigatory Powers Act 2000](#) (RIPA 2000)

12.2 The CCTV systems will be managed and operated in accordance with these Acts.

12.3 Camden Council's CCTV systems is registered with the Information Commissioners Office (ICO) for the use of CCTV systems in accordance with the Data Protection Act 1998 and will ensure that the principles of the Data Protection Act are adhered to.

12.4 Regulation of Investigatory Powers Act 2000 Covert surveillance activities of public authorities are regulated by the Regulation of Investigatory Powers Act (RIPA) 2000.

12.5 Any covert use of CCTV systems by or on behalf of a public authority and with the authority's knowledge immediately places such use within the bounds of the RIPA Act. The requirements of RIPA must be complied with at all times.

13. Information Commissioners Office (ICO) In The Picture

13.1 The [ICO CCTV code of practice – In The Picture](#) provides guidance and advice for CCTV users on how to comply with the Data Protection Act and also includes a simple checklist for users of very limited CCTV systems where the full provisions of the code would be too detailed.

14. Subject Access Request (SAR) Request for Personal Data

14.1 The [Data Protection Act 1998](#) allows individuals to have copies of any personal data held by the Council, including recorded CCTV images.

14.2 The Council may deny access to information where the act allows, particularly where it may prejudice, prevention and detection of crime or the apprehension, prosecution of offenders or the exercise of the Council's statutory functions.

14.3 Subject Access Requests (SAR) for CCTV images should be sent to:

15 Public Information

15.1 Public information for this code of practice is a public document and will be available for inspection. More information can found [HERE](#).

16 Security, Complaints and Breaches of Code

16.1 Complaints and breaches of the code including those of security will be dealt with in accordance with the Council's or the Metropolitan Police Service's complaints procedures.

The Council has a corporate complaints procedure webpage to enable users of Council services to make a complaint as well as to make other comments or compliments, which can be found on our website [HERE](#)