



THE LONDON BOROUGH
www.bromley.gov.uk

Code of Practice

CCTV

2023

Contents

1. Introduction
2. Objectives of the CCTV Systems
3. Principles
4. Protection of the Freedoms Act 2012 and the “Surveillance Camera Code of Practice” issued by the Secretary of State
5. Data Protection Act 2018, General Data Protection Regulation and the Regulation of Investigatory Powers Act 2000
6. Requests for Personal Data
7. Ownership and Management of the Systems
8. Installation
9. Management and Operation of the CCTV Systems
10. Police use of the CCTV Systems
11. Security of the CCTV Control Room and Recorded Material
12. Management of Recorded Data
13. Maintenance of CCTV Equipment
14. Assessment of the CCTV Systems and Code of Practice
15. Public Information
16. Complaints and Breaches of the Code including those of Security
- Annex 1 Guiding Principles from “Surveillance Camera Code of Practice” issued by Secretary of State 2021

Dated: September 2023

1. Introduction

LB Bromley (“the Council”) owns and operates closed circuit television systems that surveil public areas throughout the borough, its housing estates and public buildings. This Code of Practice applies to all CCTV systems owned or operated by or on behalf of the Council, whether in areas to which the public normally has access or other premises where access is restricted.

This Code is designed to ensure that the Council’s CCTV systems are managed effectively and efficiently and operated within the law. An Operating Procedures Manual supplements this Code, showing how individual systems are to be operated in accordance with the Code.

2. Objectives of the CCTV systems

- To reduce the fear of crime;
- To deter crime, detect crime and provide evidence of offences;
- To enhance community safety, assist in developing the economic wellbeing of Bromley and encourage greater use of the facilities and amenities of the borough;
- To assist the Council in its enforcement and regulatory functions;
- To assist in highways management;
- To support civil proceedings;
- To support the Bromley integrated transport policy;
- To assist the Council deliver its statutory and other functions ;
- To assist in the management of Council premises; and
- To assist the Council in its overall resilience planning linked to civil contingency planning, emergency response and business continuity functions

3. Principles

Each CCTV system will be operated fairly, within the law and in accordance with this Code.

Each CCTV system will be operated so as 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.

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 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 6, “the right to a fair hearing”.

The public interest in the operation of CCTV Systems will be maintained through the security and integrity of operational procedures.

4. Protection of Freedoms Act 2012 and the “Surveillance Camera Code of Practice” issued by the Secretary of State

The Protection of Freedoms Act 2012 and the “Surveillance Camera Code of Practice” issued by the Secretary of State in June 2013 under S.30 of the Act:

- Establish a framework for CCTV surveillance and CCTV systems.
- Strike a balance between public protection and individual privacy.

The Council and the Police must have regard to the Surveillance Camera Code of Practice and to abide by the 12 guiding principles, which are set out in **Annex 1**.

5. Data Protection Act 2018, UK General Data Protection Regulation 2021 and the Regulation of Investigatory Powers Act 2000

Data Protection Act 2018 and UK GDPR

The CCTV systems will be managed and operated in accordance with the Data Protection Act 2018 and UK GDPR 2021, see: www.ico.gov.uk.

The Council’s corporate Data Protection policies and procedures can be viewed on the Council’s web site.

The Council is registered with the ICO for the processing of personal data accordance with the Data Protection (Charges and Information) Regulations 2018 and will ensure that the principles of the Data Protection Act and GDPR are adhered to.

Regulation of Investigatory Powers Act 2000

Covert surveillance activities of public authorities are regulated by the Regulation of Investigatory Powers Act (RIPA) 2000. 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 2000 Act. The requirements of RIPA must be complied with at all times.

6. Requests for Personal Data

The GDPR allows individuals to have copies of any personal data held by the Council, including recorded CCTV images. The Council may restrict the amount of personal data it supplies when it is, 'necessary and proportionate' in order to:-

- avoid obstructing an official or legal inquiry, investigation or procedure;
- avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- protect public security or national security; or
- protect the rights and freedoms of others.

Subject access requests in respect of CCTV images are to be made using the online form on the Council's website.

Freedom of Information requests are to be made using the online form on the Council's website.

7. Ownership and Management of the Systems

The Council owns and manages the CCTV systems. It is responsible for compliance with this Code and ensuring that the rights and interests of the public and of the individual are maintained.

The day-to-day operation of the systems is the responsibility of the Council or its agents, providers contracted by the Council for such purpose.

The Council and the Metropolitan Police Service will liaise closely with regards to management of the systems, where applicable.

In compliance with the ICO's CCTV Code of Practice, all systems are to be properly signed to inform members of the public about the management and purposes of the system.

8. Installation

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 surveil those areas that are intended to be viewed by the equipment. Both permanent and movable or re-locatable cameras should be sited and image capture restricted to ensure that they do not view areas that are not of interest and are not intended to be the subject of surveillance, for instance an individual's private property. 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.

Prior to installation of a new system, the addition of a camera(s) to an existing system or the relocation of a camera or any other change to the system, a Data Protection Impact Assessment (DPIA) is to be completed, which is to include consultation with stakeholders and the community. The technical assessment for the installation is to establish clear operational requirements for the cameras or system and is to consider the benefits to be gained, whether or not other or better solutions exist and what effect it may have on individuals and their privacy and, is it justifiable in the circumstances and a proportionate response to the problem to be addressed.

From time to time re-locatable or transportable cameras may be installed temporarily. The use of such cameras and the data produced by virtue of their use, will always accord with the objectives of CCTV in Bromley and this Code.

9. Management and operation of the CCTV systems

No person, whether Council staff, Police officers, or security staff contracted to the Council for such purpose, is to operate CCTV equipment until s/he has been trained in the operation of the system and the rules and procedures relating to its operation.

The operators of the system will be required to adhere to this Code of Practice. Council and its suppliers' staff will be subject to their employer's disciplinary procedures in the event of breach of this Code and / or the operational procedures.

All use of the cameras shall accord with the purposes and key objectives of the CCTV scheme and shall comply with this Code.

Only those members of staff with responsibility for using the equipment shall have access to operating controls.

Operators of the CCTV system must act with the utmost integrity.

A requirement of confidentiality will be enforced during and after termination of employment.

In accordance with the Information Commissioner's CCTV Code of Practice (2014) and the Secretary of State's Surveillance Camera Code of Practice (2013), the systems are to be audited annually to ensure that there remains a requirement to operate the system and collect and retain personal data and to ensure that that other legal requirements, policies and standards are complied with in practice.

10. Police use of the CCTV systems

The following applies equally to the Police and other statutory investigation agencies use of the CCTV systems. 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.

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. Police use of the CCTV system, including both the review of recorded as well as viewing live images, is to be strictly controlled.

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. 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.

Any remote control and recording of cameras will strictly adhere to this Code of Practice.

11. 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.

Recorded images are to be kept securely at all times and live and recorded images are to be viewed and reviewed to meet the purposes of each system, only.

Recorded images are not to be sold or used for commercial purposes, publicity or the provision of entertainment.

Access to the Council's CCTV equipment and control room(s) is to be restricted to those managing or operating the systems, authorised users and visitors and, installation and maintenance engineers.

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 and personal data and, the time of arrival and departure.

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).

The System Operators will hold primary responsibility for ensuring that there is no breach of security and that this Code is complied with at all times. S/he will have day-to-day responsibility for the management of the Control Room and for enforcing the disciplinary code. The Systems Operator will ensure that any serious breach of this Code is duly notified in accordance with the Council's GDPR and 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. Any breaches will be subject to investigation and possible disciplinary action in accordance with the Council or its contractor's procedures.

12. Management of recorded data

Recorded material, including video stills, will be used only for the purposes defined in this Code and access to it strictly limited. Recorded material will not be sold or used for commercial purposes or the provision of entertainment.

The Council may use recorded images to promote the effectiveness of its CCTV systems.

No more images and information are to be stored other than that which is required for the stated purpose of a surveillance camera system and such images and information are to be deleted once their purposes have been discharged: for public safety systems this is 31 days, typically, though this may vary from scheme to scheme.

The showing of the recorded images to the public will only be allowed in accordance with the law: either in compliance with the needs of the Police in connection with the investigation of crime, which will be conducted in accordance with the provisions of any relevant Code of Practice under the Police and Criminal Evidence Act 1984 and any advice and guidance given to the Police from time to time; or in any other circumstances provided by the law.

Access to recorded images by the Police, other statutory investigation agencies or officers of the court is permitted under the Data Protection Act 2018, Police and Criminal Evidence Act (PACE) 1984 and the Criminal Procedures and Investigations Act 1996.

13. Maintenance of CCTV equipment

The CCTV systems are to be repaired and maintained in full working order and so as to meet the operational requirements.

14. Assessment of the CCTV Systems and Code of Practice

The Council will ensure the CCTV Systems and this Code are evaluated at regular intervals to assess crime impact on neighbouring areas without CCTV, the views of the public and the operation of this Code.

The Council officer with the day to day responsibility for CCTV will continuously monitor the operation of the CCTV system and the implementation of this Code.

15. Public Information

This Code of Practice is a public document and will be available for inspection

16. Complaints and breaches of the Code including those of security

All complaints will be dealt with in accordance with the Council's complaints procedure.

The Council's corporate complaints procedure webpage to enable users of its services to make a complaint as well as to make other comments or compliments, see:

https://www.bromley.gov.uk/info/200025/complaints/378/complaints_procedure

Email: corporate.complaints@bromley.gov.uk

Guiding Principles from the “Surveillance Camera Code of Practice” issued by the Secretary of State revised 2021

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 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.