CCTV

Code of Practice

2021

For the operation of CCTV systems owned and operated by Basildon Borough Council

Contents

Appendices

1. Introduction

This Code of Practice is set out to control the management, operation and use of all Closed-Circuit Television (CCTV) systems under the control of Basildon Borough Council, and is used in conjunction with the Home Office Surveillance Camera Code of Practice pursuant to section 29 of the Protection of Freedoms Act 2012.

Basildon BC ("the Council") own and operate public space CCTV systems 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. Operating Procedures Manuals supplement this Code, showing how individual systems are to be operated in accordance with the Code.

The CCTV system operates 24 hours a day, 365 days a year, except in cases of maintenance/upgrades, faults etc, where it may be necessary for a particular system to be powered down for a period of time.

This Code of Practice will be reviewed annually and at any time when the system has a relevant change in process, software or hardware. Any required revisions and alterations will then be made.

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 Basildon and encourage greater use of the facilities and amenities of the borough;
- To assist the Council in its enforcement and regulatory functions;
- To support civil proceedings;
- To assist the Council deliver its statutory and other functions;
- To assist in the management of Council premises and Contracts;
- To assist the Council in its overall resilience planning linked to civil contingency planning, emergency response and business continuity functions;
- To assist with staff disciplinary action as part of an internal investigation

3. Principles

Each CCTV system will be operated fairly 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:

- Establishes a framework for CCTV surveillance and CCTV systems.
- Strikes 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 in Section 2.6 which are set out in **Appendix 1** and the CCTV Policy.

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

Data Protection Act 2018 and GDPR 2016

The CCTV systems will be managed and operated in accordance with the Data Protection Act 2018 and GDPR 2016, see: www.ico.gov.uk.

The Council's corporate Data Protection policies and procedures can be viewed on the Council's website.

The Council is registered with the ICO for the processing of personal data in accordance with the Data Protection (Charges and Information) Regulations 2018 and will ensure that the principles of the Data Protection Act 2018 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. Ownership, Management & Operation of the Video Surveillance Systems

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 survey those areas that are intended to be viewed by the equipment.

Both permanent and movable or re-deployable 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, such as individuals' 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.

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 Basildon and this Code.

Dummy Cameras

Studies have shown that public confidence in CCTV is based upon effectively operating cameras, therefore dummy cameras will no longer be used within any CCTV schemes operated by the Council.

Maintenance of CCTV equipment

Effective and regular maintenance of a CCTV system is essential to ensure that the system is effective at all times.

All cameras receive two pre-planned maintenance services, which includes cleaning and testing of physical equipment.

The contractor carrying out the maintenance will have ISO 9001:2015 and work in accordance to BS7858.

Management and Operation of the CCTV 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 Essex 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.

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 the Council suppliers' staff will be subject to their employer's disciplinary procedures in the event of breach of this Code and / or 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.

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.

Live Facial Recognition Technology

The Council will not use any facial recognition technology as part of the CCTV system.

Access to the Control Room

The control room door has an access control system and will always remain secured. Routine access to the control room will be limited to duty controllers, designated officers of the Council, approved contractors, designated officers of Essex Police and police officers and police community support officers collecting evidence, undertaking approved on-going investigations and liaison visits. All persons wishing to access the CCTV control room must sign a copy of the confidentiality agreement at the commencement of and end of each visit.

The confidentially agreement reads as follows: -

"I understand that during my visit to Basildon Borough Council's CCTV control room I may observe images or hear radio conversations that may be of a confidential nature. I am aware that the Council operates a code of conduct for all its visitors to the control room which it expects to be adhered to. I have read and understood this Confidentiality and Code of Conduct agreement and I will not disclose any confidential information to another person unless I have obtained permission to do so from an authorised representative of Basildon Borough Council."

Visitors

Organised visits for viewing the operation of the system are arranged on a regular basis to promote the use of CCTV as a crime prevention tool, raise awareness and reduce the fear of crime. All visitors will be required to sign a copy of the confidentiality agreement at the commencement and end of each visit.

Visits must be arranged in advance by letter or electronic mail and may be subject to change or termination at short notice to meet operational requirements. For confidentiality purposes, the police airwave radio will remain switched off or to a low volume during visits and a telephone link will revert to be the primary source of contact with Essex Police. It is imperative that operations are managed with the minimum of disruption therefore casual visits will not be permitted.

Contractors

Access for contractors will be necessary from time to time for the purpose of maintaining existing equipment and to carry out new installations. Other Building related hardware is located in the CCTV Control Room such as the fire alarm panel and the intruder alarm panel.

All contractors are asked to sign a copy of the confidentiality agreement at the commencement of and end of each visit where access to the CCTV control room is necessary. Contractors are asked to give as much notice as possible when planning to carry out works in the control room environment to avoid any disruption to the day to day running.

Staffing of the Control Room

All Security Officers are SIA (Security Industry Authority) Public Space CCTV trained.

All Control Room staff will be employed directly by the Council or via the Council's appointed staffing contractor. All such staff will be required to pass stringent security appraisals to ensure their integrity before being employed as Control Room Operators. Day to day supervision of all Control Centre staff will be the responsibility of the nominated Supervisor/Manager.

Equipment associated with the CCTV System will only be operated by authorised personnel who will have been properly trained in its use and all control/monitoring room procedures. Each operator will be personally issued with a copy of both the Code of Practice and the Procedural Manual. They will be fully conversant with the contents of both documents, which may be updated from time to time, and which they will be expected to comply with as far as is reasonably practicable at all times.

Arrangements may be made for a Police liaison officer/s to be present in the monitoring room at certain times, subject to locally agreed protocols. Any such person must also be conversant with this Code of Practice.

7. Police 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 CCTV systems 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.

8. Security of the CCTV systems 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 only to be viewed and reviewed to meet the purposes of each system.

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 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 CCTV systems, recording the visitors' confirmation that they will maintain the confidentiality of CCTV operation and personal data and, the time of arrival and departure.

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. S/he will have day-today responsibility for the management of the CCTV equipment 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 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.

9. Management of recorded data

Recorded material will only be used for the purposes defined in this Code and access to it is 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 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: For public safety systems typically this is 31 days, though this may vary from scheme to scheme.

When footage is transferred to a disc or other portable device for a primary or secondary request to view data, the footage will be stored securely for 12 months before being confidentially destroyed.

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.

10. Requests for Data

Primary request to view data

Primary requests to view data generated by a CCTV system are likely to be made by third parties for any one or more of the following purposes:

- Providing evidence in criminal proceedings
- Providing evidence in civil proceedings or tribunals
- The prevention of crime
- The investigation and detection of crime (may include identification of offenders)
  • Identification of witnesses

Third parties, who are required to show adequate grounds for disclosure of data within the above criteria, may include, but are not limited to:

- Police
- Statutory authorities with powers to prosecute, (eg. Customs and Excise; Trading Standards, etc)
- Solicitors
- Claimants in civil proceedings
- Accused persons or defendants in criminal proceedings
- Insurances
- Other agencies, (as agreed by the Data Controller and notified to the Information Commissioner) according to purpose and legal status

Upon receipt from a third party of a bona fide request for the release of data, the data controller shall:

- Not unduly obstruct a third-party investigation to verify the existence of relevant data.
- Ensure the retention of data which may be relevant to a request, but which may be pending application for or the issue of a court order or subpoena. A time limit shall be imposed on such retention which will be notified at the time of the request.

Where requests fall outside the terms of disclosure and Subject Access legislation, the data controller or nominated representative shall:

- Be satisfied that there is no connection with any existing data held by the police in connection with the same investigation.
- Treat all such enquiries with strict confidentiality.

Secondary request to view data

For example, where a member of the public requests CCTV images of their vehicle in a car park where there has been an incident of criminal damage or a fail to stop incident.

Before complying with a secondary request, the data controller shall ensure that:

- The request does not contravene, and that compliance with the request would not breach, current relevant legislation, (eg. Data Protection Act 2018, Human Rights Act 1998, section 163 Criminal Justice and Public Order Act 1994, etc);

- Any legislative requirements have been complied with, (e.g. the requirements of the Data Protection Act 2012); Protection of Freedoms Act 2012.
- Due regard has been taken of any known case law (current or past) which may be relevant, (eg. R v Brentwood BC ex p. Peck);

- The request would pass a test of 'disclosure in the public interest'.

If, in compliance with a secondary request to view data, a decision is taken to release material to a third party, the following safeguards shall be put in place before surrendering the material:

- In respect of material to be released under the auspices of 'crime prevention', written agreement to the release of the material should be obtained from a police officer, not below the rank of Inspector. The officer should have personal knowledge of the circumstances of the crime/s to be prevented and an understanding of the CCTV System Code of Practice.

- If the material is to be released under the auspices of 'public well-being, health or safety', written agreement to the release of material should be obtained from a senior officer within the Local Authority. The officer should have personal knowledge of the potential benefit to be derived from releasing the material and an understanding of the CCTV System Code of Practice.

  Recorded material may be used for bona fide training purposes such as police or staff training. **Under no circumstances** will recorded material be released for commercial sale of material for training or entertainment purposes.

Subject Access Request

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
- protect the rights and freedoms of others

Subject access requests in respect of CCTV images should be sent to,

The Data Protection Officer
Basildon Borough Council
The Basildon Centre
St. Martin's Square
Basildon, Essex
SS14 1DL
01268 533333

Individual access to personal data of which that individual is the data subject must be permitted providing:

- The request is made in writing;
- The data controller is supplied with sufficient information to satisfy him or herself as to the identity of the person making the request;
- The person making the request provides sufficient and accurate information about the time, date and place to enable the data controller to locate the information which that person seeks, (it is recognised that a person making a request is unlikely to know the precise time. Under those circumstances it is suggested that within one hour of accuracy would be a reasonable requirement);
- The person making the request is only shown information relevant to that particular search and which contains personal data of her or himself only unless all other individuals who may be identified from the same information have consented to the disclosure.

In the event of the data controller complying with a request to supply a copy of the data to the subject, only data pertaining to the individual should be copied, (all other personal data which may facilitate the identification of any other person should be concealed or erased).

The data controller is entitled to refuse an individual request to view data under these provisions if insufficient or inaccurate information is provided, however every effort should be made to comply with subject access procedures and each request should be treated on its own merit.

In addition to the principles contained within the Data Protection legislation, the data controller should be satisfied that the data is:

- Not currently and as far as can be reasonably ascertained not likely to become part of a 'live' criminal investigation.
- Not currently and as far as can be reasonably ascertained not likely to become relevant to civil proceedings.
- Not the subject of a complaint or dispute which has not been actioned.
- The original data and that the audit trail has been maintained.
- Not removed or copied without proper authority.

- For individual disclosure only (i.e. to be disclosed to a named subject).

11. Public Information

This Code of Practice is a public document and is published on the Council website.

Some minimal information regarding CCTV locations are also published on the website.

Signage / Letting people know

The CCTV Code of Practice requires us to ensure that people are aware that CCTV is in use. Example signage can be seen in appendix 2.

Signs are required to:-

- Be clearly visible
- Be readable
- Give details of the organisation operating the system
- Show the purpose of the scheme and who to contact

12. Complaints

All complaints will be dealt with in accordance with the Council's or the Essex 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, see: www.basildon.gov.uk/complaints

13. Assessment and review of the CCTV Systems and Code of Practice

The Council will ensure the CCTV Systems and this Code are evaluated at regular intervals; not less than on an annual basis.

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.

Appendix 1

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 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.

Appendix 2


CCTV
Cameras in operation
in this area
Images are being monitored
for the purposes of
Crime Prevention & Public Safety
Tel: 01268 206874
SAFERBASILDON
BasildonCouncil