



Castle Point Borough Council

Code of Practice on the use of

CCTV

Compliant with the Surveillance Camera Code of Practice as amended November 2021

Solicitor to the Council
Castle Point Borough Council

October 2022

Review Date October 2024

The Council's Mission Statement in the use of CCTV systems – To provide a safe and secure environment in those areas covered by the CCTV System and for the benefit of all those living, working and visiting the area.

Purpose

This Code of Practice provides a common framework for the management and operation of existing and/or future CCTV schemes within the Borough of Castle Point and includes arrangements between the Police and the Borough Council to meet the requirements of legislation and regulations governing the use of CCTV. It also sets out the minimum standards required for the operation of CCTV schemes. In addition, the Council is required to have regard to the Home Office Surveillance Camera Code of Practice, pursuant to Section 33(1) of PoFA 2012.

Aims

The aims of CCTV schemes managed or operated by Castle Point Borough Council are as follows:

- The prevention and detection of crime
- To reduce incidence of nuisance, anti-social behaviour, vandalism and graffiti
- To gather intelligence and identify suspects
- The maintenance of public order
- To reduce the fear of crime
- To promote safer communities
- To improve health and safety of the police, the public and employees
- Undertake locally agreed assignments provided they adhere to current legislation and this Code of Practice
- To assist with the overall management of Council owned Public Open Spaces
- To assist with the overall management of Council owned Buildings
- To assist the Council in its enforcement and regulatory functions
- To assist in the production of evidential material for Court proceedings
- To assist in the Council with any investigation under its Disciplinary Policy and Procedure Policy
- For the detection of drowning at the Council Leisure Centres

Guiding Principles

The Council has adopted the following 12 guiding principles:

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 user 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 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.

Disclaimer

Whilst every effort will be made to monitor CCTV Systems neither Castle Point Borough Council nor Essex Police will accept any liability in respect of any incident not observed or, for any observed incident whether any response is made or not.

Intention

CCTV Systems will be used to view and record images in accordance with the objectives and principals shown above. Images will be transmitted to a secure recording/viewing environment.

When required, the system will provide the means by which evidence can be adduced by any person or body having lawful reason for accessing the recorded images, and that such evidence may subsequently be made available for court proceedings.

Specialist and covert intrusive surveillance by Police and other prosecuting agencies are not covered in this Code of Practice. In cases where such monitoring is required and which falls outside this Code, appropriate authority must be obtained in order to comply with legislation.

1. Introduction

This Code of Practice is intended to support the Council's Corporate Information Security Policy and is intended to be fully compliant with the Home Office Surveillance Camera Code of Practice. It is also intended to be compliant with the Data Protection Act 2018, Human rights Act 1998, Equality Act 2010 and the Protection of Freedoms Act 2012.

The objective of this Code of Practice is to ensure that good practice standards are adopted by those who operate CCTV on behalf of the Council and that by following its provisions assists the Council and its employees to remain within the law and foster public confidence by demonstrating that the Council takes its responsibilities in relation to the protection and security of personal information seriously.

This Code of Practice shall be reviewed at least biennially and where necessary consider any updates in the following:

- The interpretation of the provisions of the Data Protection legislation
- The changes in technology involved in recording images
- The use of such technology
- Other legislation and policies introduced to cover the use of CCTV

This Code of Practice is intended to set out how CCTV Systems are managed and operated by Castle Point Borough Council.

The covert surveillance of activities is not covered by this Code of Practice because they are governed by the Regulation of Investigatory Powers Act (RIPA) 2000. Please see the Council's Corporate Policy and Guidance on RIPA available on the Council's website www.castlepoint.gov.uk.

2. About this Code of Practice

In general, this Code of Practice provides the rules and standards required by Castle Point Borough Council for the management and operation of its CCTV Systems. The Code will be supported by Operating Procedures for the running of the schemes.

This code will ensure that Castle Point Borough Council manages its CCTV Systems ethically and fairly ensuring that it contributes to community safety by preventing and detecting crime.

An important factor in any CCTV scheme is competent staff operating the system. It is therefore a requirement of this code that they are trained and qualified to undertake CCTV operating in order to provide the best possible pictures available and maintain the integrity of the system in gathering evidence for court. CCTV images have been immensely successful in securing convictions at court and to continue this trend Castle Point Borough Council are committed to maintaining and improving high quality CCTV management and operation. This code is committed to being compliant with the Home Office Surveillance Camera Code of Practice.

Dedicated CCTV operators will not be employed so the schemes will be restricted by operational limits.

This Code of Practice applies to those persons involved in operating CCTV and other devices which capture images of identifiable individuals or information relating to individuals for any of the following purposes:

- Seeing what an individual is doing under the stated aims on page 2 of this document
- Potentially taking some action in relation to an individual, e.g. handing the images over to the police to investigate a crime
- Using the images of an individual in some way that will affect their privacy e.g. passing images on to a TV company
- Images used to investigate any wrongdoing during employment of staff or contractors

It also covers other information derived from those images that relate to individuals (e.g. vehicle registration marks).

As most CCTV is directed at viewing and/or recording the activities of individuals this means that the use of CCTV will be covered by the GDPR and the Data Protection Act 2018.

The Council's Data Controller who is legally responsible for compliance with the Data Protection Act is the Council's Strategic Director for Corporate Services Andrew Roby Smith whose contact details are:

Council Offices
Kiln Road
Benfleet,
Essex SS7 1TF
Email: asmith@castlepoint.gov.uk
Tel: 01268 882434

3. Use of CCTV or continued use of CCTV

Using CCTV can be privacy intrusive, as it is capable of putting law abiding people under surveillance and recording their movements as they go about their day-to-day activities.

Careful consideration will be given as to whether to use CCTV; the fact that it is possible, affordable or has public support should not be the primary motivating factor. The Council will take into account what benefits can be gained, whether there are better solutions that exist and what effect it may have on individuals.

Consideration of the above matters will be given objectively as part of an assessment of the CCTV scheme's impact on people's privacy. The extent of the assessment will depend on the size of the proposed scheme and the level of impact it is likely to have on people's privacy.

Results of the impact assessment will be used to determine whether CCTV is justified in all the circumstances and if so how it should be operated in practice.

As a public authority the Council must comply with its obligations under the Human Rights Act 1998, in particular Article 8 (the right to respect for private and family life, home and correspondence.) as use of CCTV may well impact on an individual's private and family life.

The Impact Assessment Questionnaire is shown in Appendix 1.

4. Potential benefits of use of CCTV in the Borough of Castle Point

Use of CCTV in the Borough of Castle Point will reassure the public and enable relevant images to be made available for use by the Police as well as relevant employees of Castle Point Borough Council to interact and view the images 24 hours per day available 7 days a week. This will include live images as well as recorded images.

Use of Council CCTV would be permitted to the Police following receipt of a complaint or request to view the relevant camera or camera footage for the subject location, observe the incident and communicate the occurrence to officers attending the scene and permit the early detection, evidencing and direction of law enforcement officers to the scene of the occurrence or perpetrator. CCTV footage will enable officers to identify offenders and inform officers allowing Police officers to make fast and informed decisions to arrest offenders and or deter future offending.

The facility to retain CCTV footage and for it to be used as evidence will also enable the police and the Council to prosecute offenders in the absence of witnesses or to corroborate witness evidence to unlawful activities. Footage will only be retained for the purposes set out in this Code and any retained footage will be deleted once the purpose of its retention has been discharged.

Use of CCTV in the Borough will assist with public reassurance, knowing that their personal safety and the protection of their property would be safeguarded and would, being overt and publicised by the local authority deter criminal behaviour and offer security to residents, reduce crime as well as obtain evidence for any subsequent proceedings or issues that may arise.

Use of a redeploy-able CCTV system allows the movement of cameras to areas as necessary to assist the Council in its aims as set out in this Code.

5. Ensuring effective administration

There must be as much transparency in the use of CCTV camera systems as possible as well as clear responsibility and accountability for all surveillance camera activities including images and information collected, held, and used. It is therefore important to establish who has day to day responsibility for the control of CCTV images to include:

- Deciding what is to be recorded,
- How the images should be used and
- To whom they may be disclosed

Access to retained images and information is restricted and the Council is ultimately responsible for any use of the information gathered under the Data Protection Act including when shared with other partner organisations. The Council and partner agencies are, for the purposes of this Code also responsible for any decisions made about the purposes and operational use of the Council's CCTV. For example, where the Police have a live feed from a local authority owned camera for a stated lawful purpose.

If the Council uses an outside partner or organisation for processing services e.g. editing images there must be a contract and data sharing agreement in place with that organisation to ensure that the images are only processed in accordance with the Council's instructions. There is a duty to have regard to the Home Office Surveillance

Camera Code of Practice and although not binding on third party service providers, any Contract entered into by the Council must have regard to the code when exercising functions to which the code relates including guarantees about security e.g. storage and use of properly trained staff.

For the purpose of this Code, authorised staff are:

- Operational Services Manager – Environment Services
- Environmental Rangers – Environment Services
- Community Safety Officer (CCTV Data Co – Ordinator) – Licensing and Safer Communities
- Head of Licensing & Safer Communities – Licensing and Safer Communities
- Leisure and Community Services Manager – Environment Services
- Health and Fitness Manager – Environment Services
- Duty Manager – Environment Services
- Office and Marketing Manager – Environment Services
- Finance Administration Officer – Environment Services
- First Contact Manager – First Contact
- Revenues & Benefits Transformation Manager – Housing and Communities
- Revenues Manager – Housing and Communities
- Team Leader (Recovery & Enforcement) – Housing and Communities
- Housing Management and Rents Manager – Housing and Communities
- Housing Management Officer – Housing and Communities
- Senior Sheltered Housing & Communities Officer – Housing and Communities
- Sheltered Housing & Communities Officer – Housing and Communities
- Temporary Accommodation Support Officer – Housing and Communities
- Housing Options Officer – Housing and Communities
- Street Scene and Contracts Manager – Environment Services
- Monitoring and Enforcement Officer – Environment Services
- Education, Enforcement and Monitoring Officer – Environment Services
- District Commander or their representative Castle Point Essex Police

For the purposes of any investigation under the Council's Disciplinary Policy and Procedure, any officer appointed to conduct an investigation by Human Resources or other authorised officer, should be properly trained and have regard to this code.

Where images are made available to the Police and other recognised bodies from Castle Point Borough Council's CCTV System, they will be bound by this Code, The Home Office Surveillance Camera Code of Practice, GDPR and the Data Protection Act 2018. This will ensure that the same high standards of security and ethics are uniformly applied to other partners in the scheme. It also safeguards the Council against potential abuse of the system and ensures the recorded material is treated in accordance with the legislation and Code of Practice. It also serves to gain the support and confidence of the public that the Council's CCTV System is being operated openly, transparently and in an ethical manner.

Where images are made available to other prosecuting agencies, it is expected that this Code and the Home Office Surveillance Camera Code of Practice will apply.

6. Discipline

A breach of any aspect of this Code, the Home Office Surveillance Camera Code of Practice or the Operating Procedure Manual (Appendix 2) by Council employees may

involve disciplinary action in accordance with the Council's Disciplinary Code and in relation to other bodies a formal Complaint made to that body.

Any breach of this Code, the Home Office Surveillance Camera Code of Practice or the Operating Procedures Manual by an employee of Essex Police or any other prosecuting authority who, for a specific purpose, has been allowed access to the System in accordance with the aims of this code will be expected to be subject of that organisation's disciplinary codes or practices and to report any such breaches where required.

7. Procedures for using CCTV

7.1 Positioning of Cameras

Use of a surveillance camera system and the location of cameras and the means by which images are captured must always be for a specific purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

Cameras should be situated where they will capture images relevant to the legitimate aim pressing need for which the scheme has been established. For example, if a camera is located for the prevention of disorder or crime, it should be capable of capturing facial images to identify suspects and/or offenders.

Individual Camera siting should take place on the basis of an operational requirement setting out the scope of each camera. Cameras should be sited in such a way as to monitor only those areas to which the public has access. However, if it is not possible physically to prevent cameras from viewing private areas, then staff must be suitably trained and made aware of the privacy implications under the Data Protection and Human Rights Acts. A DPIA should be completed for any new camera siting's to help assure compliance with obligations as data controller under the data protection legislation.

Users of the surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

Areas required to be viewed by CCTV for security or similar purposes, which the public do not have access to, are not governed directly by this code. However, material gathered for any subsequent proceedings should be dealt with in accordance with the instructions set out in this document.

Signs will be placed in the proximity of the scheme so that the public and staff are aware they are entering a zone covered by surveillance equipment. The signs will be clearly visible to the public, be an appropriate size and contain the following information;

- a) The identity of the organisation responsible for the scheme
- b) The address of the organisation
- c) The purpose of the scheme

The signage format used in this CCTV System is of A3 and A4 size dependent on positioning;

Main sign on boundaries of scheme – A3 size

Additional 'repeater' signs within scheme – A4 size

Any covert operation and / or any requirement to remove existing signs will be done so with the approval of authorised Castle Point Borough Council /Essex Police Staff and in accordance with RIPA laws and the Council's RIPA policy.

Information/images so obtained must only be obtained for the prevention and detection of criminal activity, or the apprehension and prosecution of offenders. It should not be retained for any purpose other than those indicated in the objectives of the scheme above.

The existing equipment does not record sound.

Signage for internal CCTV

Signs will be placed in the area of the internal building where the CCTV is in use so that the users of the building and visitors to the building are aware they are entering a zone covered by surveillance equipment. The signs will be clearly visible to the public, be an appropriate size and contain the following information;

- a) The identity of the organisation responsible for the scheme
- b) The address of the organisation
- c) The purpose of the scheme
- d) State whether the CCTV records sound as well as images

The signage format used in this CCTV System is of A4 size or A3 size dependent on positioning;

Bodycams

Reference must be made to the specific departments Privacy Impact Assessment and Procedural Process Document.

7.2 Quality of Images

It is important that images recorded by the equipment are of sufficient quality to be effective for the purposes for which they are made. It is essential that cameras positioned for crime detection and/or prevention should be capable of good quality images able to identify suspects and offenders.

This CCTV System and all subsequent systems have an appropriate maintenance regime so as to maintain the required quality and cameras that fail to reach the appropriate level of quality will be changed or removed from the system.

All data will be treated according to the GDPR and Data Protection Act and this Code.

Digital media will be of a suitable standard so as to ensure good quality images.

The CCTV System records details of the camera location, date and time etc.

7.3 Processing Images

Images will not be retained for longer than is necessary. Generally, evidential images will be retained under the rules of the Criminal Procedure and Investigation Act 1996. This includes unused material. Full guidelines are set out in the manufacturer's manual.

Where images are retained, no more images and information should be stored than that which is strictly required for the stated purpose of this code and such images and information should be deleted once their purposes have been discharged and will be in accordance with the objectives set out in this Code of Practice.

Images retained for these purposes will be securely stored so as to ensure their integrity is maintained. This will also ensure that the evidential value is maintained to protect the rights of members of public who may have been recorded.

Access to these images will be carefully controlled and restricted to those persons who have access under the GDPR and the Data Protection Act 2018. Images will only be released to those persons who have a legal right to view them. Images held for evidence will be documented fully in the appropriate log.

7.4 Security Policy

Access to retained images and information is restricted and security is essential and must be maintained at all times to comply with data protection legislation.

Access to monitoring will be restricted to designated/named members of staff and other authorised persons with a legitimate purpose.

Visits by Inspectors and Auditors may take place at any time accompanied by an authorised person. Any such visit will be recorded in the visitor's log.

If the need arises to evacuate the Control Centre by virtue of a security alert or fire alarm; all staff will act in accordance with local instructions.

Access to recorded images will be restricted to authorised Castle Point Borough Council Staff, System Operators and any other authorised persons.

Viewing of images will take place in a restricted area. The basis for this restriction is to protect the privacy rights of members of the public and to avoid compromising persons who view the monitors.

7.5 Technical introduction

Wireless CCTV systems allow viewing on site as well as remote monitoring from almost anywhere. It is not only possible to monitor and review cameras live on site but also to have the system monitored remotely at other times. Remote access provides the ability to view any site from any location. This facility is particularly valuable for operators who do not necessarily wish to visit sites but nonetheless need to be able to observe progress or activity.

Alternatively, images can be transmitted across Wireless LAN / Wi-Fi connection, which enables access to the camera and all its functionality from a Laptop, whilst in a 100 -200m range of the unit. This offers great flexibility for the equipment & enables it to be deployed wherever you need to locate a camera system.

When connected wirelessly using either of these methods, the system provides full remote control of the cameras (pan, tilt and zoom), configuration of pre-set positions, automatic tours and hard disk settings. Overt and covert systems explained WCCTV supplies both covert and overt systems.

All recording is retained for 30 Days on Hard drive.

7.6 Authorised staff (CCTV panel)

For the purpose of this Code authorised staff or their nominated representative's are:

- Operational Services Manager – Environment Services
- Environmental Rangers – Environment Services
- Community Safety Officer (CCTV Data Co – Ordinator) – Licensing and Safer Communities
- Head of Licensing & Safer Communities – Licensing and Safer Communities
- Leisure and Community Services Manager – Environment Services
- Health and Fitness Manager – Environment Services
- Duty Manager – Environment Services
- Office and Marketing Manager – Environment Services
- Finance Administration Officer – Environment Services
- First Contact Manager – First Contact
- Revenues & Benefits Transformation Manager – Housing and Communities
- Revenues Manager – Housing and Communities
- Team Leader (Recovery & Enforcement) – Housing and Communities
- Housing Management and Rents Manager – Housing and Communities
- Housing Management Officer – Housing and Communities
- Senior Sheltered Housing & Communities Officer– Housing and Communities
- Sheltered Housing & Communities Officer– Housing and Communities
- Temporary Accommodation Support Officer– Housing and Communities
- Housing Options Officer– Housing and Communities
- Street Scene and Contracts Manager – Environment Services
- Monitoring and Enforcement Officer – Environment Services
- Education, Enforcement and Monitoring Officer – Environment Services
- District Commander or their representative Castle Point Essex Police

7.7 Authorised staff (CCTV panel)

The Authorised staff will regularly monitor, assess and discuss the use and relevance of the deployment of CCTV cameras. All cameras will be deployed subject to the agreement of the CCTV panel where appropriate. When considering the evidence for the deployment of re-deployable CCTV and locations. Subject to specified statistical evidence available for a specific area the CCTV Panel may require one or more cameras to be applied to the location.

7.8 Installation

All equipment will be subject to the installation of a qualified person authorised by the CCTV Panel and shall be installed in accordance with the positioning guideline contained in this code.

7.9 Recording of Information

Record's will be retained by the CCTV Data Co-ordinator's of:-

- Completed Data Privacy Impact Assessments in relation to the siting of each CCTV scheme.
- Requests for information.
- Information and evidence from each request.
- All cost records and Invoicing for use of CCTV.
- All other documents the Community Safety Officer (CCTV Data Co-ordinator) considers necessary.

7.10 Retention of evidence from CCTV operation

Where evidence is obtained from a Castle Point CCTV camera, The organisation requesting this information and receiving any Data will be required to retain a copy of that information for 12 Months or for such period as agreed between the Council and the organisation, but information must not be retained for any longer period than the purpose for which it was acquired.

7.11 Request for information

All requests for information regarding Castle Point CCTV must comply with this Code of Practice.

8. Application of this Code of Practice

This Code does not apply to Essex Police or other prosecuting agencies for **specialised and covert intrusive surveillance**. In this instance, appropriate authority will be obtained under part 3 of the Police Act. Where it is necessary to carry out "Directed Surveillance"(Directed Surveillance is defined in the Operating Procedures Manual) the appropriate authority will be obtained from the relevant officer as specified in the Regulation of Investigatory Powers Act 2000.

9. Disclosure Policy

9.1 Access To and Disclosure of Images to Third Parties

Access and disclosure of retained images and information (live and recorded) will be restricted and carefully controlled to ensure the rights of individuals are preserved. This will also ensure the chain of evidence remains intact, should images be required for evidence.

Authorised Castle Point Borough Staff must ensure that access and the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

Standards;

1. Employee and staff access to recorded images is restricted to those with authorised access.
2. All access to images must be documented.

3. Access to images by third parties will only be allowed in limited and prescribed circumstances. i.e., if the purpose of the system is the prevention and detection of crime, then disclosure to third parties is limited to the following:-
 - Law enforcement agencies where the images recorded would assist in a specific criminal enquiry.
 - Agencies with a Statutory Duty of investigation. This will be judged on a case by case basis.
 - Legal representatives. This will be judged on a case by case basis.
 - The media, where it is assessed by the Police, that the public's help is needed in order to assist in the identification of a victim, witness or perpetrator in relation to a criminal incident. (See Operating Procedures Manual for process and guidance on victims wishes, Appendix 2)
 - Individuals who have been recorded and have a right of access under data protection laws (unless disclosure would prejudice a criminal enquiry or criminal proceedings)
 - Police Forces and Local Authorities where the sole purpose is to use images for the training of Police Officers, Managers and Operators.
4. All requests for access to images or requests for copies will be fully documented. If access or disclosure is denied, the reason(s) will be fully documented. Data Subject Access forms will be sent to members of the public who apply for access.
5. When access or disclosure is allowed, then the following will be documented:-
 - The date and time at which access was allowed or the date on which disclosure was made
 - The identification of any third party who was allowed access or to whom disclosure was made
 - The reason for allowing access or disclosure
 - The extent of the information (Details of camera, time, date, location etc) to which access was allowed or disclosed.
6. Recorded images will not be made available by Castle Point Borough Council on the Internet.
7. If it is intended that images are to be made more widely available, for example, in the public interest, then that decision shall be made under the direction of Essex Police in accordance with the aims of the scheme. The reason for that decision will be documented and comply with PACE (Police and Criminal Evidence Act) code of practice if applicable and:-
 - Any relevant court proceedings must have been concluded for a minimum of 28 days.

- There must be no appeal lodged or pending and no associated proceedings pending.
8. If images are released to the media (Other than in circumstances detailed above) the images of individuals or other identifying data will be disguised or blurred.
 9. If images are released to third parties, it is their responsibility to ensure compliance with the Data Protection Act and the Human Rights Act and as far as possible with the Home Office Surveillance Camera Code of Practice and an guidance from the Information Commissioners Office applicable at that time.

10. Data Subject Access Policy

10.1 Access by Data Subjects

The right of access to images of Individuals by that individual is provided for in section 7 of the Data Protection Act 1998 and should be afforded wherever possible. The processes for dealing with requests are set out in this document. but the standards below will apply:

Authorised staff must be able to recognise a request for access to recorded images by data subjects.

Data subjects can make a verbal request to view footage. Data subjects will be provided with a standard subject access request form (Appendix 3) that:-

- a. Indicates the information required to locate the images requested
- b. Indicates the information required to identify the person making the request
- c. Indicates the fee that will be charged for carrying out the search for the images requested.
- d. Asks whether the individual would be satisfied with merely viewing the images recorded.
- e. Indicates that a response will be made promptly and no longer than 40 days from the day the request was received (which will be endorsed on the form)

All subject access requests will be dealt with by an authorised member of staff. Where possible, the designated member of staff will locate the images requested.

The authorised member of staff will determine whether disclosure to the individual will entail disclosing images of third parties. Similarly, he/she will decide if the images are held under a duty of confidence. It is likely that a member of the public walking in a public area will have less expectation that their images are held under a duty of confidence than those recorded for example in a police waiting room.

If third party images are not to be disclosed, they should be disguised or blurred out as in the Disclosure Policy.

If the authorised member of staff decides that a subject request form should not be complied with, he/she will notify the applicant and a written copy of this decision will be notified within 14 days of the decision and he or she will document the following:-

- a. The identity of the individual making the request
- b. The date of the request
- c. The reason(s) for refusing to supply the images requested
- d. The name and signature of the designated member of staff making the decision.

All staff should be aware of the individuals' rights under this section of the Code of Practice.

Full local operating practice is contained in the Operating Procedure Manual (Appendix 2).

10.2 Other Individuals' Rights

The disclosure or viewing of images may cause third parties to be placed in a compromising position, depending on the content of the images. The GDPR and the Data Protection Act 2018 makes provision for other individuals' rights to be taken account of.

Section 10 of the Act provides the individual the right to prevent processing which is likely to cause damage or distress.

The following standard applies;

Castle Point Borough Council and Essex Police staff must be able to recognise a request from an individual in order to prevent processing likely to cause substantial and unwarranted damage to that individual.

All staff must be aware of the CCTV Data Co-ordinator who is responsible for responding to such requests

The Head of Law or their authorised member of staff will:-

- a. Document fully any response to a request where processing is likely to cause damage or distress and whether it will be complied with or not.
- b. Provide a written response to the individual within 21 days setting out the decision and reasons.
- c. Retain a copy of the response to the individual.
- d. If such an appeal is received, then again within 21 days a response will be made setting out the steps being taken to deal with the individuals' appeal.

The CCTV Data Co-ordinator or authorised member of staff shall document the following:-

1. The original decision
2. The request from the individual
3. The response to the request from the individual

11. Compliance Monitoring

This CCTV System will comply with this Code of Practice. There will be a system of monitoring in place to ensure:-

- Compliance with these Codes of Practice as well as the Home Office Surveillance Camera Code of Practice
- Public support for the scheme is maintained
- Continued ethical use of the system
- Best value

The contact point indicated on the signs within the area covered by CCTV should be available to members of the public at least during office hours. The following information will be available at the Council's Main Office in Kiln Road:

How to obtain Access to a copy of the Codes of Practice

Subject access request form

Details of the complaint procedure

Castle Point Borough Council will monitor the effectiveness of the CCTV system and set out recommendations for any improvements or changes, so as to ensure the scheme complies with the stated purpose, objectives and aims through the CCTV Panel. Castle Point Borough Council will review complaints and praise in order that compliance with legal obligations and provisions with this Code of Practice can be monitored.

12 Complaints procedure

All complaints will be dealt with in accordance with CPBC existing complaints procedure.

Appendix 1
Impact Assessment Questionnaire

Question	Answer
Who will take responsibility for day to day management and security of the CCTV images?	
What is the purpose for using CCTV? What are the problems it is meant to address?	
What are the benefits to be gained for the use of CCTV?	
Can CCTV technology realistically deliver these benefits? Can less privacy-intrusive solutions e.g. improved lighting, achieve the same objectives?	
Do you need images of identifiable individuals, or could the scheme use other images not capable of identifying the individual?	
Will the particular equipment/system of work being considered deliver the desired benefits now and remain suitable in the future?	
What future demands may arise for wider use of images and how will you address these?	
What are the views of those who will be under surveillance?	

What could you do to minimise intrusion for those that may be monitored, particularly if specific concerns have been expressed?	
Human Rights considerations: <i>(if your response is in the negative to one or more of the questions below then it would not be appropriate to use CCTV)</i>	
Is the proposed system established on a proper legal basis and operated in accordance with the Law:	
Is it necessary to address a pressing need, such as public safety, crime prevention or national security?	
Is it justified in the circumstances?	
Is it proportionate to the problem that it is designed to deal with?	
Equality Impact considerations:	

Appendix 2

Operating Procedure Manual

The CCTV Systems covered by this Code will have in place a Manufacturers Operating Procedure Manual setting out the day to day guidelines for operating the system. The Code of Practice will contain local instructions and policy and ensure that manufacturers operating instructions are complied with.

A manual will be maintained and updated to document when processes or camera positions change, including changes to the camera specification. This will be the responsibility of a Manager or a designated member of staff. This Operating Procedure Manual is not available to the public.

Any major change in the operating manual should be discussed and agreed at an appropriate level. Minor changes may be agreed locally by authorised Council Staff or the CCTV Data Co-ordinator in accordance with the Code of Practice.

Training

All authorised staff will be trained to an agreed level. This will assist in the implementation of these Codes of Practice and ensure that evidence gathered will be of a suitable quality.

Health & Safety

At no time will unqualified staff undertake maintenance or interfere with equipment other than in accordance with the guidelines issued by manufacturers for normal operating procedures.

Where contractors carry out maintenance on CCTV equipment within the Castle Point Borough Council District, the contractor will complete a report with the start and finishing time they are on the premises and a brief description of the work carried out.

At no time will staff be expected to carry out duties that would bring them into conflict with Health and Safety regulations.

Appendix 3

Subject Access Request

Subject Access

If you wish to exercise your rights of subject access as provided for in the GDPR and the Data Protection Act 2018 while a request can be made verbally it will assist the Council if request could be made in writing on a 'Subject Access Request Form'. All requests for subject access must be received within 7 days and submitted on the appropriate form. They will be dealt with by a member of the Authorised Staff via the Data Co-ordinator for the Castle Point Borough Council CCTV System. A written response to the request will be provided within 14 days of receipt, either setting out the steps intended to be taken to comply with the request or reasons for refusing the request. In any case, all attempts will be made to finalise any request for information within 1 month.

Application Access Forms are available from the Council offices, Kiln Road, Benfleet, Essex, SS7 1TF

These notes explain how you can find out what information, if any is or maybe held about you on the CCTV System.

Your Rights

Subject to certain exemptions, you have a right to be told whether any personal data is held about you. You also have a right to a copy of that information in a permanent form except where the supply of such a copy is not possible or would involve disproportionate effort, or if you agree otherwise. Castle Point Borough Council will only give that information if it is satisfied as to your identity. If release of the information will disclose information relating to another individual(s), who can be identified from that information, the Castle Point Borough Council is not obliged to comply with an access request unless

- The other individual has consented to the disclosure of information, or
- It is reasonable in all the circumstances to comply with the request with or without the consent of the other individual(s)

Castle Point Borough Council CCTV System

Castle Point Borough Council may deny access to information where the Act allows. The main exemptions in relation to information held on the CCTV System are where the information may be held for –

- Prevention and detection of crime
- Apprehension and prosecution of offenders

And giving you the information may be likely to prejudice any of these purposes.

The Application Form:

Data is held for 28 days

Please be aware that application forms which we receive 28 days after the request date (the day for which you are requesting information from the CCTV system) cannot be processed.

(N.B. ALL sections of the form must be completed. Failure to do so will delay the processing of your application)

- | | |
|------------------|--|
| Section 1 | Asks you to give information about yourself that will help us to confirm your identity. We have a duty to ensure that information we hold is secure and we must be satisfied that you are who you say you are. |
| Section 2 | Asks you to provide evidence of your identity by producing TWO official documents (which between them clearly show your name, data of birth and current address) together with a recent full-face photograph of you. |
| Section 3 | Asks you to specify the form of information required (viewing only or viewing/permanent copy) |
| Section 4 | The declaration should be signed by you. |
| Section 5 | Asks you to give details in order to assist with locating the information. |
| Section 6 | Gives details of where you may obtain further information. |

When you have completed and checked this form, take it or send it together with the required TWO identification documents, photograph:

**Data Co-ordinator
Community Safety Department
Council offices
Kiln Road
Benfleet
Essex
SS7 1TF**

The Data Protection Act 2018

Section 1 about Yourself

The information requested below is to help us (a) satisfy ourselves as to your identity and (b) find any information held about you

PLEASE USE BLOCK LETTERS

Title (Tick box as appropriate)	Mr		Mrs		Miss		Ms	
Other Title (e.g. Dr, Rev, etc)								
Surname/Family Name								
Maiden Name/Former Name								
Sex (tick box)	Male				Female			
Height								
Personal Description (please inform us of any other personal features which might help us to identify you)								
Date of Birth								
Place of Birth	Town							
	County							

Your Current Home Address (To which we will reply)		
	Post code	

Telephone Number (Home)	
Telephone Number (Work/Mobile)	

If you have lived at the above address for less than 1 year, please give your previous addresses for the period:

Previous Address(es) (Include dates of occupancy)	
---	--

Section 2 Proof of Identity

To help establish your identity your application must be accompanied by TWO official documents that between them clearly show your name, date of birth and current address (these **must** be originals).

For example: a birth certificate, driving licence, medical card, passport, utility bill or other official document that shows your name and address.

Also, a recent full face photograph of yourself.

Failure to provide this proof of identity will delay the processing of your application

Section 3 Supply of Information

You have a right, subject to certain exceptions, to receive a copy of the information in a permanent form.

I wish to:

View the information only / View the information and receive a permanent copy*

*Please delete as appropriate

Section 4

Declaration

WARNING – a person who impersonates or attempts to impersonate another may be guilty of an offence.

Note that all requests made which are related to a possible criminal act can only be processed via the police and not the data subject. The incident **must** be reported to the police. CCTV footage of this nature will only be made available if the police deem it to be appropriate.

Please explain the reason(s) for this data subject access request

Declaration, signature and date

Section 5 Locating the Information

Locating information can be very difficult. Please be as specific as you can when completing the below questions so that you may be identified more easily.

Date and **exact** time

--

Exact location

--

Clothing worn

Any other information (To assist identification. E.g. pushing pram, holding shopping bag etc)

NOW – Check application and enclosed documentation against ‘CHECK’ Box before returning form.

CHECK BOX

Have You:

- Completed ALL Sections on this form?
- Enclosed TWO identification documents?
- Signed the declaration and dated the form?

Section 6

Data Protection Act 2018

Further Information:

The information contained at the front of this form is to be regarded as a guide only. Full details can be found in the Data Protection Act 2018, which is obtainable from The Stationery Office at the following address:

**Enquiries
HMSO
St.Clements
2-16
Norwich
NR3
0870 600 5522**

**House
Colegate

1BQ**

Further information and guidance may be obtained from:

**Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF**

Tel: (01625) 545745

Please note that this application for access to information must be made to Castle Point Borough Council at the previously stated address and **NOT** to the Data Protection Commissioner.

OFFICIAL USE ONLY

Please complete all of this section

Application checked and legible?	<input type="checkbox"/>	Date application received	<input type="text"/>
Identity documents checked	<input type="checkbox"/>	Fee Paid	<input type="text"/>
		Receipt Number	<input type="text"/>
		Date Docs. returned	<input type="text"/>
Details of I.D. documents	<input type="text"/>		
Member of staff completing this section:			
Name	<input type="text"/>	Department.	<input type="text"/>