Brentwood Borough Council

Public Space C.C.T.V Surveillance System

Code of Practice
2024

Whilst the content of both documents are accurate at the time of publication, differences and alterations to laws of evidence and procedural matters may arise.
The content of either or both documents are not intended to form a contract.
Neither Brentwood Borough Council nor the Essex Police can accept liability for any error or omission; or for the advice, guidance or information contained within either the Code of Practice or the associated Procedures Manual.

Foreword

Public Space CCTV systems have become increasingly popular across the UK. It has possibly become one of the most powerful tools to be developed over recent years to assist with efforts to combat crime and disorder whilst enhancing community safety. Equally, it may be regarded by some as the most potent infringement of peoples' liberty.

Brentwood Borough Council and its partners are committed to the belief that everyone has the right to respect for his or her private and family life and their home. They also believe that there should be no interference by any public body with the exercise of this right except such as is may be in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals or for the rights and freedoms of others.

Therefore as a public authority it is vital that at all times we follow the guidance in relation to the current CCTV legislation and ensure full compliance with a persons' right to privacy whilst at the same time working within the community safety partnership towards a strategic vision for our borough.

We are pleased that over the years during which our CCTV has been in place it has proven to be an essential tool and that working in partnership we can have an impact on the prevention of crime and disorder. We feel certain that it will provide a secure and safe environment for those who visit, work or live in Brentwood Borough Council as we also want to encourage growth and unlock potential for our residents.

This Code of Practice and the associated Procedures Manual have been developed in conjunction with The Surveillance Camera Commissioners CCTV code of practice which provides 12 guiding principles on what is considered to be CCTV best practice. Recommendations from the Protection of Freedoms Act 2012 in relation to CCTV have also been taken into account.

An integral part of any CCTV system is a code of practice which sets out the objectives for CCTV and how the system will work and be controlled. We hope that this Code of Practice will as far as is reasonably possible give the public confidence in the system and how it is operated. In particular, it aims to ensure that issues such as privacy and the integrity of the system are properly managed and maintained at all times.

Contents

For the purpose of this document,
Where the terms '**Council**' or '**BBC**' are used this is to mean

Town Hall
Ingrave Road
Brentwood
Essex
CM15 8AY

The ‘owner’ of the system is Brentwood Borough Council.

For the purposes of the Data Protection Act, the ‘data controller’ is Brentwood Borough Council.

The ‘System Manager’ is Brentwood Borough Council.

The Scheme is registered under the Data Protection Act 1998.

As the owners of the Closed Circuit Television System (hereafter referred to as CCTV), the Council has overall responsibility for maintaining and managing the system, in doing so it will also ensure commitment through compliance with this Code of Practice

This Council is in partnership with the:

Essex Police,
Police Headquarters
Springfield
Chelmsford
Essex
CM2 6DA

There is a Glossary provided at the end of this code of practice to assist with the understanding of phrases, terminology and legislature used throughout this document.

Introduction

The Council has made significant investment in its CCTV provision across the borough. We have 84 public space cameras which are monitored 24 hours a day, 365 days a year by a team of experienced and licensed operators.

These Systems are in place in the town centres of Brentwood, Shenfield and Ingatestone and at other strategic locations across the borough such as outside of railway stations and community spaces. All cameras are in what is known as public space, Public Space cameras are also utilised for traffic management and enforcement purposes.

There are cameras located for the protection of the Town Hall and there are also a further 20+ cameras located in and around council owned blocks including in lifts and at their access and egress points.

CCTV was introduced into the Borough and it has undergone many transitions and changes. Not only from public awareness and understanding, technical developments, and changes of legislative requirements in relation to Human Rights and the Protection of Freedoms Act but through to funding available to enable us to manage and maintain these systems continually proactively.

CCTV has many virtues and is an essential tool but for it to continue to flourish there is a requirement for acceptance of the benefits it can afford us rather than concerns that it is an invasive entity which we would rather not have.

There are more cameras on the streets than before but they have all been erected for specific purposes of Crime and Antisocial Behaviour and environmental enforcement. Many are dual purpose and serve both roles. All have been erected for specific purposes having gone through a process that is adopted by our Community Safety Tasking which involves four distinct areas of assessment which are Evaluation, Environment, Enforcement and justification for having cameras in situ. This process for deployment undertaken by Brentwood Borough Council ensures compliance with this code of practice. Process has been through Consultation with the Community Safety Partnership, Corporate Leadership Team and the relevant committee.

This Code of Practice has been drawn up to govern the activities of the system and its operators. The code incorporates advice and guidance issued by the Home Office through its Surveillance Camera Code of Practice 2013 on the effective use of surveillance camera systems to relevant authorities (as defined by Section 33 of the 2012 Act) issued by the Secretary of State under Section 30 of the Protection of Freedoms Act 2012

The Council is committed to continually maintaining, reviewing and improving the scheme as appropriate whilst working within this Code of Practice.

The recorded data in the various systems used remain the property of the owner of that particular system.

The copyright of all recorded material, whether analogue or digitally stored, remains totally with Brentwood Borough Council.

No recorded material will be sold or used for commercial purposes or the provision of entertainment.

Objectives of the Code of Practice

The main objectives of this Code of Practice are:-

- To satisfy the community over the competence and honesty of the system and its operators.

- To ensure that staff are aware of and follow the correct procedures in the case of an 'incident'.

- To ensure that recorded evidence is retained in such a way as to fulfil the requirements of the Crown Prosecution Service.

- To reassure the community over the privacy in private areas and domestic buildings.

- To ensure that all data obtained is done so fairly within the law, and only for the purpose for which the system has been established.

- To ensure the public interest in the operation of the system is recognised through the security and integrity of operational procedures.

- Develop commitment to sustaining the efforts of measures taken.

The Code addresses the issue of responsibility, monitoring, procedures, governing of staff, the handling of recorded data and Control Room access.

Changes in this code will fall into two categories.

- MAJOR: - these will only be carried out after full consultation with all relevant parties.

- MINOR: - these will be completed only after agreement of the Senior Representatives of all partners concerned.

Purpose of CCTV in Brentwood Borough Council

The primary purpose of the CCTV system in place for Brentwood Borough Council is to provide a safe town environment for those who live, work, trade or are visiting the area.

It is anticipated that the system will as far as reasonably practicable: -

- Enhance community safety by reducing the fear of crime and encouraging greater use of the Town Centre's, shopping centre, car parks and public spaces.
- Help with the detection and prevention of crime.
- Facilitate in the apprehension and prosecution of offenders in the relation to crime and public disorder.
- Provide the police, the council and other parties with evidence to take criminal and civil action in the courts.
- Monitor the service delivery of the Council.
- Reduce nuisance, antisocial behaviour, and vandalism.
- Within this broad outline the Partnership may draw up key objectives which would be based on current local concerns and reviewed on a regular basis.
- Environmental Enforcement, including flytips and littering.

It should be noted that the system is intended to view activity in public areas only. It will not be used to invade the privacy of any persons in domestic, business, or other private premises, buildings, or land. Recording and monitoring equipment will be programmed to ensure safeguards are put in place where necessary (such as Privacy Zones/Pixelation), to prevent cameras being focused on people's homes, gardens or other private property and instructions to operators in relation to this matter are implicit. (This section does not apply to the rear yard and Control Room systems).

Throughout this Code of Practice it is intended, to offer a balance between the objectives of the CCTV System and the need to safeguard the individual's right to privacy as set out by the Protection of Freedoms Act 2012. Throughout the Code every effort has been made to indicate that a formal structure has been put in place, (including a complaints procedure) by which it should be identified that the System is not only accountable but is seen to be accountable.

This Code of Practice (hereafter referred to as 'the Code') will be supplemented by a separate Procedures Manual which offers instructions on all aspects of the operation of the system. To ensure the purpose of the CCTV system is realised, the manual is based upon the contents of the Code.

Description of CCTV Systems

Types of Cameras

1. Overt

All cameras installed in the current systems are “overt” in nature. This implies that all are clearly visible and in all cases will have a sign noting the presence of a camera on the column on which it is mounted. They are located within shopping areas, principal highways, pedestrian thoroughfares, and residential estates.

2. Covert

A covert camera by design is one that is constructed to blend in with its surroundings so as to avoid detection. These are usually mobile and re-deployable by nature. The use of such cameras and the data produced by virtue of their use will always be in accord with the objectives of the CCTV System.

The activity being investigated by a covert camera would normally be of such a nature that normal policing methods are inappropriate.

No camera either covert or overt will be operated in a covert fashion without reference to the Regulation of Investigatory Powers Act 2000 as outlined in the Procedures Manual. If an operator receives any request to operate the system in a manner that would fall under the remit of ‘Directed Surveillance’ the appropriate level of authority will be obtained before any activity takes place.

- Cameras are mixed in shape and size. They can either be a rectangular box shape known as a ‘shoebox camera’ or domed either as a camera set in a dome or as a camera which is spherical by design.

- Cameras will be full colour, Pan, Tilt and Zoom (PTZ) or full colour static (which do not have the ability to move) and are normally placed on a fixed objective such as (but not excluded to) in a lift or on a doorway.

- Mobile or re-deployable cameras either record locally (at the camera) or utilise a number of different transmission methods to enable onward transmitting of images.

- Camera positions have been carefully evaluated and planned to provide maximum coverage whilst, at the same time, minimising the effect on individual privacy. Every effort will be made to ensure that all ‘incidents’ are recorded.

Primary Control

Only those authorised members of staff with responsibility for using the CCTV equipment will have access to the operating controls, those operators always have primacy of control.

Secondary Control

Limited secondary monitoring and control facilities are being arranged in partnership with Essex Police. This will be a managed process and can only be carried out after authorisation and in all cases control and monitoring will be administrated and recorded in accordance with this Code of Practice and the Procedures Manual.

The CCTV Control Room also has a direct radio link via Airwave Radio to Essex Police.

All cameras are owned by the Council.

Operation of the System by the Police

Under operational circumstances the Police may make a request to assume control of a camera/s from the CCTV system to which this Code of Practice applies. Only requests made on the written authority of a police officer not below the rank of Superintendent will be considered. Any such request will only be accommodated on the personal written authority of the most senior representative of the system owners (or designated deputy of equal standing).
In the event of such a request being permitted, the CCTV Control Room will continue to be staffed and equipment operated by only those personnel who are authorised to do so.
In very extreme circumstances a request may be made for the Police to take total control of the scheme in its entirety, including the staffing of the control room and personal control of all associated equipment to the exclusion of all representatives of the system owners.
Any such request will only be considered personally by the most senior officer of the scheme owners (or designated deputy of equal standing). A request for total exclusive control must be made in writing by a police officer not below the rank of Assistant Chief Constable or Deputy Commissioner (or person of equal standing).
Any such operations may come under the provisions of the Regulation of Investigatory Powers Act 2000[1].

[1] See Appendix D

Recording Equipment

Under normal circumstances the recording of images will be facilitated by Brentwood Borough Council CCTV digital video recording system. This is self contained within the CCTV Control Room Comms Room.[2]

Transmission of Images

Various methods are employed to transmit images across the CCTV system from the cameras to the recording facility. These include but are not limited to:

Internet Protocol (IP), Fibre Optic (Fibre), Microwave and Cabled.

Microwave transmissions are WPA2 protected at the point of transmission by password encryption.

Maintenance of the System

The System shall be maintained in accordance with the requirements of the Procedures Manual under a maintenance agreement.

ANPR System

An ANPR (Automatic Number Plate Recognition) system is in place and maintained under the guidance of the Procedures Manual.

[2] See Recording Policy.

Public Information

Public Concern

Although the majority of the public at large may have become accustomed to 'being watched', those who do express concern do so mainly over matters pertaining to the processing of the information, (or data) i.e. what happens to the material that is obtained?

All personal data obtained by virtue of Brentwood Borough Council CCTV System shall be processed fairly and lawfully and, in particular, shall only be processed in the exercise of achieving the stated objectives of the system. In processing personal data there will be total respect for everyone's right to respect for his or her private and family life and their home.

The storage and security of the data will be strictly in accordance with the requirements of the Data Protection Act 1998 and any additional locally agreed procedures.

Dummy cameras will not be used.

No sound will be recorded in public places.

Signs

Signs will be displayed throughout the area covered by CCTV to inform people of the presence of cameras. The following wording will be used in overt camera areas:

"CCTV in Operation"

All signs carry the Brentwood Borough Council, Safer Brentwood and the Essex Police Logo. In addition, all signs carry a Council Contact Number.

Accessing the Code of Practice:

A copy of this Code of Practice will be made available to anyone requesting it. Additional copies will be lodged at public libraries, Brentwood Police Station, and the Town Hall and will also be available as an electronic document on the councils' website.

CCTV Annual Report

The annual CCTV Performance Review Report and that for subsequent years shall be published by the end of April. This will be a report on the calendar year and will contain statistical and other relevant information. A copy of the annual report will also be made available to anyone requesting it. Additional copies will be lodged at public libraries, Brentwood Police Station, and the Town Hall and will also be available as an electronic document on the councils' website.

Overall Responsibility and Accountability

The following named parties are responsible for managing the system:

Brentwood Borough Council has nominated the Community Safety and CCTV Manager to manage this system.

In practice, this will be the responsibility of the Community Safety and CCTV Manager who will handle the day to day management and will have unrestricted personal access to the CCTV Control Room.

Corporate Director

Communities and Health

Tracey Lilley

Corporate Manager

Corporate Manager, Community Safety

Jonathan Woodhams

Community Safety and CCTV Manager

Daniel Cannon

Audits

The system will be subject to audits by Brentwood Borough Council Auditors, (or nominated deputy whose organisational level of responsibility is at least equal to that of the Community Safety and CCTV Manager, but who is not the Community Safety and CCTV Manager).

Audits will be undertaken on a sufficiently regular basis to provide an effective safeguard for the system.

An audit will pay particular attention to those parts of the System which are intended to address individual privacy.

Any discrepancies or concerns must be brought to the attention of the system manager who will ensure appropriate action is taken.

System Partners

System partners, including TfL and the Police, will comply with this Code.

Additionally the Police will comply with the Essex Police Code and give an account of doing so.

The Police have obtained an agreement on provision for communication and mutual exchange of information about the system and for reports from both the Council and the Police on compliance with the Code.

The Police will satisfy the Council that systems have been introduced to monitor and audit the participation of the Police in the system including compliance with the Code.

Evaluation and Review

An assessment process is to be undertaken whenever the development or review of the CCTV system is being considered to ensure that the purpose of the system is and remains justifiable, there will be consultation with those most likely to be affected, and the impact on their privacy is assessed and any appropriate safeguards can be put in place.

The System will periodically be independently evaluated to a format approved by The Home Office to establish whether the purposes of the system are being complied with and whether the specified objectives are being achieved.

Evaluations are conducted by the BBC Community Safety Partnership Strategy Group and Community, Environment and Enforcement Committee who meet with the purpose of;

1. To annually review the provision of public space CCTV to ensure it continues to meet the requirements of the community, the Council and partner agencies.
2. To ensure that all fixed and mobile CCTV is being used cost effectively and to its full advantage by reviewing, monitoring and continuing to investigate new and developing technology solutions, including but not limited to vehicle mounted cameras, body cameras and Automatic Number Plate Recognition (ANPR) cameras.
3. To work in partnership with retailers, licensees and businesses to improve the feelings of safety and reduce opportunities to commit crime in shopping areas across the Borough.
4. To ensure CCTV installed in council managed housing estates reduces opportunities for crime and anti-social behaviour and makes residents and their visitors feel safer.

To enable the delivery of the CCTV Strategy Aims, an annual Delivery Plan will be published with the Annual CCTV Performance Review.

Privacy Impact Assessment

Cameras at all times will be operated in accordance with the Protection of Freedoms Act 2012 which has a recommendation for a Privacy Impact Assessment (PIA) to have been carried out on each camera.

The aim of the PIA is to ensure that privacy risks are minimised while allowing the aims of the scheme to be met whenever possible.

A PIA also helps assure compliance with obligations under the Data Protection Act.

Brentwood Borough Council have devised and implemented an assessment process that is appropriate and proportionate to this boroughs needs[3].

[3] See Appendix H

Management of CCTV Operations

CCTV Control Room

1. Access

Normal access to the Control Room will be restricted and controlled by the CCTV Control Room staff. The site in which the Control Room is situated will be subject to CCTV Surveillance. An overt camera will ensure the security of equipment and personnel on the site. The controlled entrances to the site will have conspicuous signs stating:

"CCTV in operation"

These will not be repeated elsewhere.

- The Control Room will be secure with the approaches to them being constantly monitored.
- Movement in and out of the CCTV Control Room will be recorded in the CCTV Control Room Entry Log.
- Visits to the Control Room will be subject to the approval of the BBC Community Safety and CCTV Manager. This will entail establishing criteria for visitor approval.
- For reasons of security and confidentiality, access to the CCTV Control Room is restricted in accordance with this Code of Practice. However, in the interest of openness and accountability, anyone wishing to visit the room may be permitted to do so, subject to the approval of, and after making prior arrangements with, the Community Safety and CCTV Manager.
- Visits by inspectors or auditors may take place at anytime, without prior warning. No more than two inspectors or auditors will visit at any one time. Inspectors or Auditors will not influence the operation of any part of the system during their visit. The visit will be suspended in the event of it being operationally inconvenient.
- Regardless of their status, all visitors to the CCTV Control Room including inspectors and auditors will be required to sign the CCTV Control Room Entry Log and accept the declaration of confidentiality.
- Visitors entering the CCTV Control Room will be presented with a clearly displayed sign before entry stating the above[4].

[4] See Appendix A

2. Security

- Authorised personnel will normally be present at all times when the equipment is in use.
- If the CCTV Control Room is to be left unattended for any reason it will be secured. In the event of the CCTV Control Room having to be evacuated for safety or security reasons, the provisions of the Procedures Manual will be complied with.

3. Use of Equipment

- Only trained and authorised personnel will operate any of the equipment located within the CCTV Control Room or equipment associated with the CCTV System.
- All monitoring stations and PC's may not be manned on a 24 hour basis.
- Unmanned monitoring stations and/or PC's must be left secure and all operator controls logged off or switched of as required.

4. Equipment Demonstration

A demonstration of the capabilities and limitations of the cameras should be strictly controlled during the course of any visit with no emphasis being placed on any individual, group of individuals or property.

5. Staffing

- Brentwood Borough Council have designated; authorised and trained staff to operate the CCTV system.
- Staff have responsibility for operating the cameras, monitoring the screens, responding to events and handling recorded images including their storage and identification for evidential purposes[5].
- Sufficient staff will be on duty to ensure that the CCTV system is fully functional at all times (24 hours/day, 7 days/week).
- Suitable rest periods will be given to staff to allow maximum attention to be given to monitoring of screens.
- Any person operating the cameras will act with utmost probity at all times.
- All staff operating the system will be vetted and subject to rules of confidentiality.
- Every individual with any responsibility under the terms of this Code of Practice and who has any involvement with the CCTV System to which they refer, will be required to sign a declaration of confidentiality[6].
- All staff will be clearly instructed in their responsibility and role in operating CCTV.
- Every person involved in the management and operation of the system will be personally issued with a copy of both the Code of Practice and the Procedures Manual; and will be required to sign a confirmation that they fully understand the obligations adherence to these documents places upon them and that any breach will be considered as a disciplinary offence.

[5] Staff Responsibilities
[6] See Appendix F

- They will be fully conversant with the contents of both documents, which may be updated from time to time, and which he / she will be expected to comply with as far as is reasonably practicable at all times[7].
- Any breach by staff of this Code of Practice will result in disciplinary action.
- Any serious breaches will be treated as gross misconduct.
- Every individual with any responsibility under the terms of this Code of Practice and who has any involvement with The System to which they refer, will be subject to Brentwood Borough Council Disciplinary Procedure.
- Any breach of this Code of Practice or of any aspect of confidentiality will be dealt with in accordance with those discipline rules.
- All CCTV Control Room and associated staff will be fully trained to deal effectively with CCTV.
- Training will be given in accordance with Council procedures and a 6 month probationary period will apply.
- Only fully trained and licensed staff will be permitted to work in the CCTV Control Room.
- All CCTV operational staff are required to be SIA trained and pass Community Safety Accreditation as well as other training to ensure the appropriate level of knowledge of legislation and to ensure compliance with legislation for CCTV evidence data recording, monitoring, viewing and retrieval.[8]
- The responsibility for staff training will rest with the Community Safety and CCTV Manager. Training records will be kept for all staff.
- All personnel involved with the system shall receive supplemental training from time to time in respect of all legislation appropriate to their role.
- As an addition to any other training required or given, staff will need to undergo the Essex Police Vetting process to allow them to operate the Police Airwaves Radio system.
- The Community Safety & CCTV Manager will accept primary responsibility for ensuring there is no breach of security and that the Code of Practice is complied with. He/she has the day-to-day responsibility for the management of the room and for enforcing the discipline rules.
- All use of the cameras will accord with the purposes and objectives of the system and shall comply with this Code.
- The cameras, control equipment, recording and reviewing equipment shall at all times only be operated by persons who have been trained in their use and the legislative implications of their use.
- Cameras will not be used so as to look into private property. ‘Privacy zones’ will be programmed into the system as required ensuring that the interior of any private residential property within range of the system is not surveyed by the cameras.
- As part of their training, camera operators will be mindful of exercising prejudices which may lead to complaints of the system being used for purposes other than those for which it is intended. The operators may be required to justify their interest in, or recording of, any particular individual, group of individuals or property at any time by virtue of the audit of the system or by the Community Safety & CCTV Manager.
- Arrangements may be made for a police liaison officer to be present in the monitoring room at certain times, or indeed at all times, subject to locally

[7] Staff awareness of policy
[8] Operational standard requirement

agreed protocols. Any such person must also be conversant with this Code of Practice and associated Procedures Manual.

Health & Safety

- Control Room staff will be required to have a working knowledge of the Health and Safety at Work Act 1974 (as amended) and be aware of their responsibilities in relation to both their own and colleagues Health and Safety at work in respect of the CCTV Control Room and the council workplace, the provisions of which must be complied with at all times.
- The Control Room has been ergonomically designed to provide staff with a suitable environment and proper equipment for monitoring CCTV.
- A Rest Room, Toilet, Shower and Kitchen area are available for staff breaks at all times.
- A delegated member of staff has responsibility for all Health & Safety issues and regular inspections are carried out by the Council's Health & Safety Team.

Procedures and Policies

- A CCTV Control Room Procedures Manual, listing duties, responsibilities and the procedures to be followed, will be available at all times.
- Instructions regarding the use of equipment, with particular regard to the individual privacy of residents adjacent to the system, will be given.
- A duty roster will be published and a record of previous duties maintained and available for inspection.
- It is important that the precise details of all incidents should be recorded with accuracy.
- A record of all 'incidents' and the actions taken; will be maintained and retained using the Incident Reporting Tool available.
- CCTV related incidents will be recorded onto the relevant incident reporting tool available via the CCTV operating System (known as 'Synergy' in the current software utilised for CCTV monitoring)
- All daily activities which may assist with any subsequent enquiries will be recorded in the Daily Occurrence Log.
- Handing over of Control Room responsibility, at any time, will be recorded on the 'Shift Handover/Takeover Sheet'
- Cameras and Recording equipment will be checked during each shift to ensure that they are in good working order.

Responding to Incidents

Where ‘incidents’ identified by the CCTV system are passed to the Police for action (or vice versa), the level of response will be decided by the Police. The criteria used for responding to calls for Police attendance will generally be followed.

Police responding to ‘incidents’, in the actual vicinity of the CCTV system, will be informed that the ‘incident’ is being monitored live. Police will be informed that live recording is taking place and that “footage” of the incident is available and being kept on the system.

The BBC CCTV Control Room operator in control of these images must establish that identical pictures to those being viewed are monitored by the Police and that they are notified that they are being recorded.

Operators must ensure that live evidential images are always changed to a spot monitor to ensure that the images are captured at the highest possible frame rate available.

At the end of an ‘incident’, where it is intended that the master recorded data is to be secured as evidence, the Police Controller will dispatch an officer to request the images be downloaded onto an appropriate medium, collect the medium and appropriate statements identifying the items as exhibits.

In the event that the size of a download is such that a CD or DVD is not suitable the police will be responsible for the supply of a suitable medium for example a digital hard drive - at all times this will be at the discretion of the CCTV Manager.

Management of Recorded Material

For the purposes of this Code 'recorded material' means any material recorded by, or as the result of, technical equipment which forms part of Brentwood Borough Council Closed Circuit Television System, but specifically includes images recorded digitally, or on videotape or by way of video copying, including video prints.

Every recording used in conjunction with Brentwood Borough Council CCTV System has the potential of containing material that has to be admitted in evidence at some point during its life span.

Members of the community must have total confidence that information recorded about their ordinary everyday activities by virtue of the system, will be treated with due regard to their individual right to respect for their private and family life.

It is therefore of the utmost importance that every media of recorded material is treated strictly in accordance with this Code of Practice and the Procedures Manual from the moment it is delivered to the CCTV Control Room until its final destruction.

- Every movement and usage will be meticulously recorded.
- Access to, and the use of, recorded material will be strictly for the purposes defined in this Code of Practice only.
- Recorded material will not be copied, sold, otherwise released or used for commercial purposes or for the provision of entertainment.

Recording Policy

- All images are recorded digitally and retained for a period of no greater than 31 days unless required for a request under the Data Protection Act, Freedom of Information Act, the Police and Criminal Evidence Act 1984 or the Criminal Procedures and Investigations Act 1996.
- Subject to the equipment functioning correctly, CCTV recordings from fixed cameras are managed and maintained in the secure CCTV Control Room, which has air locked, video access control.
- CCTV recording equipment is contained in an additional secure storage area within the CCTV Control Room. Access to this area is for authorised personnel by appointment only and all callers are authenticated prior to entry and required to sign in and out of the premises.
- Recorded Material is stored on standalone Network Video Recorders (NVRs).
- The system is supported by an Uninterrupted Power Supply (UPS) and generator; these are programmed to maintain a power supply to essential equipment in the event of total power failure.
- The NVRs will be checked to ensure that the system is fully functional at the beginning of the each shift during the day.
- Spot monitors provide recordings at 25frames per second (fps) which is known as ‘real time’ this ensures no detail should be lost from an image. All images from all cameras are recorded 24hr per day (only spot monitors provide recorded images at 25fps).
- Hard disk capacity is fundamental to frame rate therefore under normal, non-incident recording, a frame rate of between 6fps and 12fps is used to maximise storage capacity.
- A time and date generator is available on the recording equipment and is always used.

Viewing Recorded Material

- A separate area with appropriate viewing equipment will be maintained close to, or as part of the CCTV Control Room. It will be supervised by control room staff, to allow for a general scanning of recorded images to take place.
- A record must be made in the Download Sheet of all action taken and details of persons viewing. The reasons for the viewing must also be defined. No unauthorised viewing must take place. The viewing of images will result in the Download Sheet reflecting the fact that such viewing has taken place.
- Investigation of all video recordings involving crime will fall under the Criminal Procedures and Investigations Act of 1996. This Act specifically refers to investigation being carried out by Police Officers. Viewing of material from the system will not be undertaken without the 'Investigating Officer' being present.

Using and Storing of Recorded Material

The digital storage of recorded images for an incident may later result in that incident becoming evidence for the Court or other proceedings. There must be proof of continuity of handling these images and their transference to a further medium from its introduction into the Control Room to its production at Court. A strict procedure needs to be in place ensuring that the evidence can be used.

1. Discs / Video Tapes / Hard drives - Provision & Quality

To ensure the quality of the downloaded images, and that recorded material will meet the criteria outlined by current Home Office guidelines; the only removable media to be used with the system are those which have been specifically provided in accordance with the Procedures Manual.

2. Discs / Video Tapes / Hard drives - Retention

Data downloaded on a removable medium will be retained for a period of 28 Days. Recorded Material will only be used in accordance with the Procedures Manual. At the conclusion of their life within the CCTV System, or when the evidence contained thereon is no longer required, they will be destroyed.

3. Network and Digital Video Recorders – Retention

Data downloaded on the fixed storage facilities will be retained for a period of six years. Recorded Material will be used in accordance with the Procedures Manual. At the conclusion of their life within the CCTV System, or when the evidence contained thereon is no longer required, they will be destroyed.

4. Discs / Video Tapes / Hard drives - Recorded Material Register

Downloaded images on any media will have a unique Download Reference number maintained in accordance with the Procedures Manual, which will be retained on the "Recorded Material Register" for at least three years after the recorded material has been destroyed. The download reference shall identify every use, and person who has viewed or had access to the recorded material.

5. Evidential Discs / Video Tapes / Hard drives

In the event of a CD/DVD/Tape or Hard drive being required for evidential purposes, the process outlined in the Procedures Manual will be strictly complied with.

6. Digital Prints

Each time a print is made it must be capable of justification by the originator who will be responsible for recording the full circumstances under which the print is taken in accordance with the Procedures Manual.

Video prints contain data and will therefore only be released under the terms of Appendix B to this Code of Practice - Release of data to third parties.
If prints are released to the media (in compliance with Appendix B), in an effort to identify alleged offenders or potential witnesses, full details will be recorded in accordance with the Procedures Manual.

A record will be maintained of all video print productions in accordance with the Procedures Manual. The recorded details will include: a reference number, the date, time and location of the incident, date and time of the production of the print and the identity of the person requesting the print (if relevant).

Complaints Procedure

In the first instance, anyone who wishes to complain about any aspect of the CCTV system or service should set out their complaint either by phone, email or in writing to:

Community Safety & CCTV Manager,
Community Safety
Town Hall,
Ingrave Road,
Brentwood.
CM15 8AY
Daniel Cannon

If you are still not satisfied with the answer you receive, make a formal complaint to Brentwood Borough Councils complaints department:

Complaints
Brentwood Borough Council
Town Hall
Brentwood. CM15 8AY
01277 312500
enquiries@brentwood.gov.uk

Glossary

Antisocial Behaviour: Any act or acts by any person(s) or group(s) which may or may not be unlawful; that affects or creates a fear or apprehension to other person(s) which is detrimental to safety and normality in or for that area.

Audit: Periodic, systematic examination of recorded material and records to review compliance with operational procedure and the Code.

CD: Compact Disc – removable data storage - usually 700 MB capacity.

Digital Prints / Video Prints / Hard Copy: A Digital print (or "Hard Copy") is a copy of an image or images which already exist on a computer disc / video.

DPIA: A Data Protection Impact Assessment is a process used to identify and assess the risks associated with processing personal data.

DVD: Digital Versatile Disc, Digital Video Disc - removable data storage - usually 4.7GB capacity.

DVR: Digital Video Recorder – a device or program that facilitates recording of digital video footage to mass storage devices.

Evaluation: Independent assessment and appraisal of the CCTV system.

HD / HDD / Hard Drive: A computer storage device either onboard a computer or as an external unit and can be of varying sizes. Increasingly, external hard drives are used for their large storage capacity.

Kilobyte = A multiple of the unit byte for digital information.

KB = Kilobyte = 1024B

MB = Megabyte = 1024KB

GB = Gigabyte = 1024 MB

TB = Terabyte =1024 GB

PB = Petabyte = 1024 TB

Monitor: Routine and continuous checking and observation.

NVR: Network Video Recorder – Software program that allows the recording of digital video footage from a network to mass storage devices.

Owner: Brentwood Borough Council which is the organisation with overall responsibility for managing the system.

Operator: An individual responsible for operating the camera controls and other CCTV Control Room equipment.

Partnership: A local partnership will contain a range of local bodies, the Local Authority, the Police, businesses, the Chamber of Commerce and others may also be involved.

Pixelation: To display an image as a small number of large pixels, typically in order to disguise someone's identity.

PC: Personal Computer.

PTZ: Pan, Tilt & Zoom - these are facilities on particular cameras allowing (where possible) the camera to move; left and right – Pan; up and down – Tilt; through 360degrees. The Zoom is a lens facility which enables the lens to move in and out, this means the camera can maintain image control and quality over a large distance.

Recorded Material: Any material recorded by, or as the result of, technical equipment which forms part of the BBC CCTV System, but specifically includes images recorded digitally, or by way of video copying, including video prints, video tapes, compact discs, digital video discs, removable or fixed computer disks, or film; any media on which images are recorded and can be reconstituted later.

System: The Technical equipment used in a CCTV system.

Tape / VHS / Video tape: A large cassette carrying varying capacity of tape. Not used much these days. Video recorders are no longer in mass production.

Relevant Legislature

Crime and Disorder Act 1998: The Crime and Disorder Act 1998 gave local authorities in England and Wales the responsibility to formulate and implement a strategy to reduce crime and disorder in their area. A key part too many of these strategies has been the installation and/or up grading of CCTV systems.

Criminal Justice and Public Order Act 1994: This Act creates the power for local authorities to provide CCTV coverage of any land within their area for the purpose of crime prevention or victim welfare.

Criminal Procedures and Investigations Act 1996: This Act requires disclosure of video evidence to defendants.

Data Protection Act 1998 (DPA): The DPA applies to the processing of personal data by data controllers. Personal data includes data that can be used on its own or in conjunction with other information likely to be in, or to come into, the possession of the same controller, to identify an individual.

The Data Controller: is the person who (either alone or jointly or in common with other persons) determines the purpose for which and the manner in which any personal data are, or are to be processed.

Freedom of Information Act 2000: This Act provides the public with access to certain information held by public authorities.

Human Right Act 1998: The European Convention on Human Rights (ECHR) Article 8 protects an individual's right to respect for a private and family life. Consequently where a CCTV system is operated by or on behalf of a public authority, the authority will also need to consider wider human rights issues and in particular the implications of ECHR Article 8.

Police and Criminal Evidence Act 1984: Codes of Practice issued under the Act detail how exhibits, such as CCTV images, used for investigations have to be handled so that they are admissible in court.

Private Security Industry Act 2001: This Act outlines a system for the statutory regulation of the private security industry.

Protection of Freedoms Act 2012: This Act outlines a system for the destruction, retention, use and other regulation of certain evidential material. It provides for a code of practice about surveillance camera systems. It also makes provisions about the release and publication of datasets held by public authorities and to make other provisions about freedom of information and the Information Commissioner.

Regulation of Investigatory Powers Act 2000: Covert CCTV surveillance is regulated under this Act by the Office of the Surveillance Commissioner.

Direct Surveillance: When an overt CCTV system is used to follow a specific, known individual in a planned operation, this has been classed as 'directed surveillance' and also comes under RIPA.

The Office of Surveillance Commissioners (OSC): Oversees the conduct of covert surveillance and covert human intelligence sources by public authorities in accordance with the Police Act 1997 and the Regulation of Investigatory Powers Act 2000 (RIPA).

Transport Act 2000 and Traffic Management Act 2004: These Acts require certification of equipment used for civil traffic enforcement devices such as CCTV to monitor bus lanes. The Acts are enforced by the Vehicle Certification Agency on behalf of the Secretary of State for Transport. The agency has published detailed Codes of practice for CCTV enforcement systems.

Appendix A

Confidentiality Clause

WARNING

ACCESS TO THIS AREA IS RESTRICTED

Everyone, regardless of status, entering this area is required to complete an entry in the CCTV Control Room Entry Log

Visitors are advised to note the following confidentiality clause and entry is conditional on acceptance of that clause

Confidentiality clause:

"In being permitted entry to this area you are acknowledging that the precise location of the CCTV Control Room is, and should remain, confidential.

You agree not to divulge any information obtained, overheard or overseen during your visit"

An entry accompanied by your signature in the Entry Log is your acceptance of these terms

Appendix B

National Standards for the release of Data to third parties under Data Protection and/or Freedom of Information Requests

If you need any more information about this or any other aspect of Freedom of Information, please Contact us – see website www.ico.org

(I) Introduction

After considerable research and consultation, the following guidance has been adopted as a nationally recommended standard by the Standards Committee of The CCTV User Group and the Local Government Information Unit in consultation with CMG Consultancy. Brentwood Borough Council has adopted these recommendations and they are reprinted in the following paragraphs.

II General Policy

a) Local procedures in place to ensure a standard approach to all requests for the release of data. Every request is to be channelled through the data controller.

The data controller is the person who (either alone or jointly or in common with other persons) determines the purpose for which and the manner in which any personal data are, or are to be, processed. In the case of Brentwood Borough Council this person is the System Manager.

III Primary Request to View Data

a) 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:

i) Providing evidence in criminal proceedings (e.g. Police and Criminal Evidence Act 1984, Criminal Procedures & Investigations Act 1996, etc.);

ii) Providing evidence in civil proceedings or tribunals

iii) The prevention of crime

iv) The investigation and detection of crime (may include identification of offenders)

v) Identification of witnesses

b) Third parties, which should be required to show adequate grounds for disclosure of data within the above criteria, may include, but are not limited to:

i) Police

ii) Statutory authorities with powers to prosecute, (e.g. Customs and Excise; Trading Standards, etc.)

iii) Solicitors

iv) Plaintiffs in civil proceedings.(3)

v) Accused persons or defendants in criminal proceedings

vi) Other agencies who fall within those categories outlined in that part of this document which identifies the purpose of CCTV Brentwood Borough Council.

c) Upon receipt from a third party of a bona fide request for the release of data, the scheme owner, Data Controller, should:

i) Not unduly obstruct a third party investigation to verify the existence of relevant data.

ii) Ensure the retention of data which may be relevant to a request.

d) In circumstances outlined at note (3) below, (requests by plaintiffs, accused persons or defendants) the owner (or nominated representative) should:

i) Be satisfied that there is no connection with any existing data held by the police in connection with the same investigation.

ii) Treat all such enquiries with strict confidentiality.

Notes

(1) The release of data to the police may not be restricted to the civil police but could include, (for example) British Transport Police, Ministry of Defence Police, Military Police, etc.

(2) Aside from criminal investigations, data may be of evidential value in respect of civil proceedings or tribunals. In such cases a solicitor, or authorised representative of the tribunal, should be required to give relevant information in writing prior to a search being granted. In the event of a search resulting in a requirement being made for the release of data, such release will only be facilitated on the instructions of a court order or subpoena.

(3) There may be occasions when an enquiry by a plaintiff, an accused person, a defendant or a defence solicitor falls outside the terms of disclosure or subject access legislation. An example could be the investigation of an alibi. Such an enquiry may not form part of a prosecution investigation. Defence enquiries could also arise in a case where there appeared to be no recorded evidence in a prosecution investigation.

(4) Brentwood Borough Council has declared that the purposes of this scheme will also include the monitoring of the Council Service delivery. Traffic Management and reduction of nuisance and vandalism; the council may release data obtained to assist in these matters.

IV Secondary Request To View Data

a) A ‘secondary’ request for access to data may be defined as any request being made which does not fall into the category of a primary request. Before complying with a secondary request, the Data Controller should ensure that:

I) The request does not contravene, and that compliance with the request would not breach, current relevant legislation, (e.g. Data Protection, section 163 Criminal Justice and Public Order Act 1994, etc.);

ii) Any legislative requirements have been complied with, (e.g. the requirements of the Data Protection Act);

iii) Due regard has been taken of any known case law (current or past) which may be relevant, (e.g. R v Brentwood BC ex p. Peck) and

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

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

i) 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.

ii) 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 the Divisional Director of Community Safety and Public Protection. 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.

c) 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.

Notes

(1) 'Disclosure in the public interest' could include the disclosure of personal data that:

i) Provides specific information which would be of value or of interest to the public well being

ii) Identifies a public health or safety issue

iii) Leads to the prevention of crime

(2) The disclosure of personal data which is the subject of a 'live' criminal investigation would always come under the terms of a primary request, (see III above).

V. Individual Subject Access under Data Protection legislation

a) Under the terms of Data Protection legislation, individual access to personal data, of which that individual is the data subject, must be permitted providing :~

i. The request is made in writing;

ii. The Data Protection Officer has been consulted and is satisfied that the request is valid and disclosure would be compliant with Data Protection Legislation

iii. The Data Controller is supplied with sufficient information to satisfy themselves as to the identity of the person making the request;

iv. 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)

v. The person making the request is only shown information relevant to that particular search and which contains personal data of themselves only, unless all other

individuals who may be identified from the same information have consented to the disclosure;

b) In the event of the scheme owner 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).

c) Brentwood Borough Council is entitled to refuse an individual request to view data under these provisions if insufficient or inaccurate information is provided. The Council will however endeavour to

Ensure that every effort is be made to comply with subject access procedures. Each request will be treated on its own merit.

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

i. The Data Controller should be satisfied that the release of the data would not prejudice the prevention or detection of crime, or the apprehension or prosecution of a defender;
ii. The Data Protection Officer should be consulted in these circumstances before any decision is taken to withhold or release;
iii. The original data and that the audit trail has been maintained;
iv. Not removed or copied without proper authority;
v. For individual disclosure only (i.e. to be disclosed to a named subject)

VI Process of Disclosure:

a) Verify the accuracy of the request;

b) Replay the data to the requester only, (or responsible person acting on behalf of the person making the request);

c) The viewing should take place in a separate room and not in the control or monitoring area. Only data which is specific to the search request should be shown

d) It must not be possible to identify any other individual from the information being shown, (any such information should be blanked-out, either by means of electronic screening or manual editing on the monitor screen)

e) If a copy of the material is requested and there is no on-site means of editing out other personal data, then the material will be sent to an editing house for processing prior to being sent to the requester.

Note

(1) Brentwood Borough Council is likely to breach Data Protection legislation if a person making a subject access request is able to identify any other individual from the information being disclosed. However a television image is two dimensional and the majority of CCTV schemes do not have immediate access to the necessary technology to blank out or remove ‘other data’. It is recommended that the advice of the Information Commissioners Office is sought in respect of any method which it is proposed should be adopted.

VII Media disclosure

The decision of Brentwood Borough Council Elected Members is that no material will be released to the press. However should circumstances arise when such release is considered essential then set procedures for release of data to a third party should be followed,

If the means of editing out other personal data does not exist on-site, measures should include the following:

a) In the event of a request from the media for access to recorded material, the procedures outlined under 'secondary request to view data' should be followed. If material is to be released the following procedures should be adopted:

i) The release of the material must be accompanied by a signed release document that clearly states what the data will be used for and sets out the limits on its use.

ii) The release form should state that the receiver must process the data in a manner prescribed by the data controller, e.g. specify identities/data that must not be revealed

iii) Proof of editing must be passed back to the data controller, either for approval or final consent, prior to its intended use by the media (protecting the position of the data controller who would be responsible for any infringement of Data Protection legislation and Brentwood Borough Council Code of Practice);

iv) The release form should be considered a contract and signed by both parties.

Notes

In the well publicised case of R v Brentwood Borough Council, ex parte Geoffrey Dennis Peck, (QBD November 1997), the judge concluded that by releasing the video footage, the Council had not acted unlawfully. A verbal assurance that the broadcasters would mask the identity of the individual had been obtained. Despite further attempts by the Council to ensure the identity would not be revealed, the television company did in fact broadcast footage during which the identity of Peck was not concealed. The judge concluded that tighter guidelines should be considered to avoid accidental broadcast in the future.

VIII Principles

In adopting this national standard for the release of data to third parties, it is intended, as far as reasonably practicable, to safeguard the individual's rights to privacy and to give effect to the following principles:

a) Recorded material should be processed lawfully and fairly and used only for the purposes defined in the Code of Practice for Brentwood Borough Council CCTV scheme;

b) Access to recorded material should only take place in accordance with this Standard and the Code of Practice;

c) The release or disclosure of data for commercial or entertainment purposes should be specifically prohibited.

Appendix C

Data Protection

1. Data Protection Legislation

The Brentwood Borough Council CCTV System is registered with the Information Commissioners Officer (ICO) in accordance with current Data Protection legislation.

The 'data controller' for The System' is Brentwood Borough Council and the day-to-day responsibility for the data will be devolved to the Community Safety and CCTV Manager.

The Community Safety and CCTV Manager is nominated as the point of contact.

All data will be processed in accordance with the principles of the Data Protection Act, 1998

Security measures to prevent unauthorised or accidental access to, alteration, disclosure, or loss and destruction of, information and/or personal data, are in place.

The system is registered under, and will be operated with due regard to, the Data Protection Act. The ICO has confirmed that all purposes stated in this document are covered by this registration.

All "data shall be processed fairly and lawfully."

Data obtained will only be processed in the exercise of achieving the stated objectives of the system. In processing personal data there will be total respect for everyone's right to respect for his or her private life and their home.

'Processing' means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including;

i. organisation, adaptation or alteration of the information or data;
ii. retrieval, consultation or use of the information or data;
iii. disclosure of the information or data by transmission, dissemination or otherwise making available, or
iv. alignment, combination, blocking, erasure or destruction of the information or data All data will be processed in accordance with the principles of the UK General Data Protection Regulation, in summarised form, includes, but is not limited to;

I. All personal data will be obtained and processed fairly and lawfully.
II. Personal data will be held only for the purposes specified.
III. Personal data will be used only for the purposes, and disclosed only to the people, shown within this code of practice.
IV. Only personal data will be held which are adequate, relevant and not excessive in relation to the purpose for which the data are held
V. Steps will be taken to ensure that personal data are accurate and where necessary, kept up to date.
VI. Personal data will be held for no longer than is necessary.
VII. Individuals will be allowed access to information held about them and, where appropriate, permitted to correct or erase it.
VIII. Procedures will be implemented to put in place security measures to prevent unauthorised or accidental access to, alteration, disclosure, or loss. and destruction of, information.

2. Request for information (subject access)

Any request from an individual for the disclosure of personal data which he / she believes is recorded by virtue of the system will be directed to the system manager, (or data controller).

The provisions of Article 15 of the UK General Data Protection Regulation (Right of Access by the Data Subject) should be followed in respect of every request.

Any request from an individual for the disclosure of personal data which he / she believes is recorded by virtue of the system must be submitted in writing.

These should be submitted to the Data Protection Officer

By email to dpa@brentwood.gov.uk

Or in writing

Data Protection Officer

Brentwood Borough Council

Town Hall

Brentwood

CM15 8AY

More information is available at https://www.brentwood.gov.uk/information-about-you#:~:text=to%20get%20information-,Subject%20access%20request,make%20a%20subject%20access%20request.

Any person making a request must be able to satisfactorily prove their identity and provide sufficient information to enable the data to be located.

The process for responding to FOI requests by e-mail:

- All responses will be sent from the Data Protection Officer.
- Your response is sent to the team completed and ready for e-mailing.
- Once they have e-mailed the customer, they will then close the record.

3. Exemptions to the Provision of Information

In considering a request made under the provisions of Article 15 of the UK General Protection Regulation, reference may also be made to Schedule 2 Part 1 (2) of the Data Protection Act 2018 which includes, but is not limited to, the following statement:

Personal data processed for any of the following purposes:

- The prevention or detection of crime
- The apprehension or prosecution of offenders

are exempt from the subject access provisions in any case to the extent that the application of those provisions would be likely to prejudice any of these matters

NB: Each and every application will be assessed on its own merits and general ‘blanket exemptions’ will not be applied.

Appendix D

Regulation of Investigatory Powers Act Guiding Principles

Advice and Guidance for Control Centre Staff and Police Inspectors in respect of CCTV and the Regulation of Investigatory Powers Act 2000

RIPA - Introduction

The Regulation of Investigatory Powers Act 2000 (hereafter referred to as 'the Act') came into force on the 2nd of October 2000. It places a requirement on public authorities listed in Schedule 1; Part 1 of the act to authorise certain types of covert surveillance during planned investigations.

The guidance contained in this Code of Practice serves to explain and highlight the legislation to be considered. A more detailed section will be included in the Procedures Manual to assist users in the application of the requirements.

RIPA - Background

General observation forms part of the duties of many law enforcement officers and other public bodies. Police officers will be on patrol at football grounds and other venues monitoring the crowd to maintain public safety and prevent disorder. Officers may also target a crime "hot spot" in order to identify and arrest offenders committing crime at that location. Trading standards or HM Customs & Excise officers might covertly observe and then visit a shop as part of their enforcement function to verify the supply or level of supply of goods or services that may be liable to a restriction or tax. Such observation may involve the use of equipment to merely reinforce normal sensory perception, such as binoculars, or the use of cameras, where this does not involve systematic surveillance of an individual. It forms a part of the everyday functions of law enforcement or other public bodies. This low-level activity will not usually be regulated under the provisions of the 2000 Act.

Neither do the provisions of the Act cover the normal, everyday use of overt CCTV surveillance systems. Members of the public are aware that such systems are in use, for their own protection, and to prevent crime. However, it had not been envisaged how much the Act would impact on specific, targeted use of public/private CCTV systems by 'relevant Public Authorities' covered in Schedule 1: Part of the Act, when used during their planned investigations.

The consequences of not obtaining an authorisation under this Part may be, where there is an interference by a public authority with Article 8 rights (invasion of privacy), and there is no other source of authority, that the action is unlawful by virtue of section 6 of the Human Rights Act 1998 (Right to fair trial) and the evidence obtained could be excluded in court under Section 78 Police & Criminal Evidence Act 1978

The Act is divided into five parts.

Part ll is the relevant part of the act for CCTV.

It creates a system of authorisation for various types of covert surveillance. The types of activity covered are “intrusive surveillance” and “directed surveillance”.

RIPA - “Covert Surveillance” Defined

Covert Surveillance is defined as observations which are carried out by, or with, the use of a surveillance device.

Surveillance will be cover where it is carried out in a manner calculated to ensure that the person or persons subject to the surveillance are unaware that it is, or may be, taking place.

RIPA - Part II - Surveillance Types

It is useful to differentiate in this guidance between “Intrusive” surveillance (which will be a great rarity for CCTV operations) and “Directed” surveillance which will be more likely.

“Intrusive” Surveillance

This is a highly invasive type of covert surveillance, the like of which CCTV equipment and their images alone would not be able to engage in except on the most rare occasion. The Act says:

“Intrusive surveillance” is defined as covert surveillance carried out in relation to anything taking place on residential premises or in any private vehicle.

This kind of surveillance may take place by means either of a person or device located inside residential premises or a private vehicle of the person who is subject to the surveillance, or by means of a device placed outside which consistently provides a product of equivalent quality and detail as a product which would be obtained from a device located inside.

Therefore it is not intrusive unless the camera capabilities are such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

The CCTV cameras installed in the Borough of Brentwood are deemed incapable of providing this level of detail so as to be considered “intrusive” for the purposes of the Act. Current interpretations re: sustained gathering of images of persons in a car in a car park dealing in drugs; being able to see clearly inside the car, would not be considered “intrusive” under the Act.

In particular, the following extract from Section 4 of this Code prevents us from carrying out intrusion of premises with cameras. This Section puts us in a strong position to resist the use of public cameras in this way by investigators.

Cameras will not be used to look into private residential property. Where the equipment permits it, 'Privacy zones' will be programmed into the system as required; ensuring that the interior of any private residential property within range of the system is not surveyed by the cameras. If such 'zones' cannot be programmed the operators will be specifically trained in privacy issues.

"Directed" surveillance

This level of covert surveillance is likely to be engaged more by public/private CCTV users when they are requested by "authorised bodies" (see later) to operate their cameras in a specific way; for a planned purpose for operation; where 'private information' is to be gained.

The Act says:

"Directed surveillance" is defined in subsection (2) as covert surveillance that is undertaken in relation to a specific investigation or a specific operation which is likely to result in the obtaining of private information about a person (whether or not specifically identified for the purposes of the investigation or operation);

and otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance.

In this section "private information" in relation to a person, includes any information relating to his private or family life.

If the BBC CCTV System is carrying out normal everyday observations by operating a particular camera to gain the best information; albeit it may not be the most obvious camera to use, or the nearest to the incident being observed, that use will not deemed to be "covert" under the terms of the Act; it is using modern technology to the advantage of the operator. It will only be where CCTV cameras are to be used in a planned, targeted way to gain private information that the requirements of authorised directed surveillance need to be met.

If the BBC CCTV System is requested to operate their cameras as part of a planned operation where the subject is aware that targeted surveillance is, or may be, taking place, "private information" is to be gained and it involves systematic surveillance of an individual or individuals (whether or not the target of the operation) then a RIPA "Directed Surveillance" authority must be obtained.

RIPA Authorisations:

Intrusive surveillance can only be "authorised" by chief officers within UK police forces and H.M. Customs & Excise and is therefore irrelevant for any other authority or agency. It is an area of RIPA that CCTV users can largely disregard.

As from the 1st of November 2012 local authorities are required to obtain judicial approval prior to using covert techniques. Local Authority authorization and notice under RIPA (Regulations of Investigatory Powers Act 2000) will only be given once an order has been granted by a Justice of the Peace in England and Wales. (Sections 37 and 38 of the Protection of Freedoms Act 2012 amended RIPA came into force on 1 November 2012)

In addition, from that date Local Authority use of directed surveillance under RIPA will be limited to the investigation of crimes which attract a six month or more custodial sentence, with the exception of offences relating to the underage sale of alcohol and tobacco. (The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 [SI 2010/521] will be amended by the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 [SI 2012/1500] on 1 November 2012.)

Police Forces - A police force maintained under section 2 of the Police Act 1996 (police forces in England and Wales). The prescribed level is a Superintendent; for urgent cases an Inspector.

The impact for staff in Police control rooms and CCTV monitoring centres, is that there might be cause to monitor for some time a person or premises using the cameras.

In most cases, this will be an immediate response to events or circumstances.

In this case, it would not require authorisation unless it were to continue for some time.

The RIPA Code of Practice suggests some hours rather than minutes.

In cases where a pre-planned incident or operation wishes to make use of public/private CCTV for such monitoring, an authority will almost certainly be required from the appropriate person within the authorised agency.

The ‘authority’ must indicate the reasons and should fall within one of the following categories:-

An authorisation is necessary on grounds falling within this subsection if it is necessary-

a) in the interests of national security;
b) for the purpose of preventing or detecting crime or of preventing disorder;
c) in the interests of the economic well-being of the United Kingdom;
d) in the interests of public safety;
e) for the purpose of protecting public health;
f) for the purpose of assessing or collecting any tax, duty, levy or other imposition contribution or charge payable to a government department; or
g) for any purpose (not falling within paragraphs (a) to (f) which is specified for the purposes of this subsection by an order made by the Secretary of State.

Every RIPA authority must be thought through and the thought process clearly demonstrated and recorded on the application. Necessity and Proportionality must be fully considered; asking the questions: “is it the only way?”, “what else have I considered?” It should not be a repeat of principles - in order to prevent & detect crime or in the interests of public safety etc.

Whenever an authority is issued it must be regularly reviewed as the investigation progresses and it must be cancelled properly upon conclusion. The completion of these stages will be looked at during any inspection process.

In cases where there is doubt as to whether an authorisation is required or not, it may be prudent to obtain the necessary authority verbally and then later in writing using the forms.

Forms should be available at each CCTV monitoring centre and are included in the procedures manual.

RIPA policing examples:

RIPA Inspector Authorisation

An example of a request requiring Inspector authorisation might be where a car is found in a car park late at night and known to belong to drug dealers. The officers might task CCTV to watch the vehicle over a period of time (no longer response to immediate events) and note, who goes to and from the vehicle - sustained surveillance of individual(s) gaining private information.

Amendment Reference S I 2003 No 3171

Which provides that there is only one ground upon which a local authority may justify covert surveillance as necessary - namely for the prevention or detection of crime and/or disorder. Additional grounds (public health, safety, etc.)

RIPA Superintendent Authorisation

Where crime squad officers are acting on intelligence linked to a long term, planned operation and they wish to have a shop premises (which is suspected of dealing in stolen goods) monitored from the outside over a period of days.

RIPA No Authorisation Required

Where officers are on patrol and come across a local drug dealer sitting in the town centre/street. It would not be effective for them to remain in a shop doorway and wish to have the cameras monitor them instead, so as not to divulge the observation taking place (Response to immediate events).

Appendix E

Confidentiality Agreement

Brentwood Borough Council

CCTV Control Room

CONFIDENTIALITY AGREEMENT

I ……..... am an employee of the Brentwood Borough Council, employed in the Community Safety and Public Protection Service. I manage, operate and monitor the CCTV surveillance cameras situated in various locations around the Borough. I have received training and understand the need for confidentiality in these matters. I am also aware that all issues dealt with in the CCTV Control Room are subject to strict rules of disclosure.

I accept that all recording media and subject material thereon are the sole property of the Brentwood Borough Council. I also understand that the copyright of the subject material contained within any of these media is retained by the Borough.

I have received and understood instructions that the material contained within the CCTV Control Room and recorded on to any media could be the subject of the Data Protection Act and subject of any current legislation brought into force. I understand that such material may be the subject of enquiries from a variety of agencies. I undertake to abide by the rules of confidentiality, outlined in the training I have received, at all times.

I accept that I will not discuss the content of these recorded materials or other confidential matters handled in the CCTV Control Room without prior knowledge and consent of the Borough, in these circumstances the Community Safety & CCTV Manager. I accept that this restriction will apply during and following my period of service with the Borough.

Employee	Witnessed on Behalf of BBC
Print Name ……..…..……..…	Print Name…….....…….....……
Signature…….…..….....	Signature……...…..……..

Appendix F

Community Safety Partnership Agreement

Operation of Brentwood Borough Council CCTV System
Agreed by:

Community Safety Partnership

Certificate of Agreement

The content of this Code of Practice is hereby approved in respect of Brentwood Borough Council Closed Circuit Television System and, as far as is reasonably practicable, will be complied with by all who are involved in the management and operation of the System.

Signed for and on behalf of
Brentwood Borough Council

Signature: .....

Name: …… Position held: ……..……

Dated the: ..... day of..... 20.....…

Signed for and on behalf of:
Essex Police

Signature: .....

Name: …… Position held: ……..……

Dated the: ..... day of..... 20.....…

Appendix G

Data Protection Impact Assessment

1. INTRODUCTION

A Data Protection Impact Assessment (DPIA) is a process used to identify and assess the risks associated with processing personal data and the measures and controls that can be applied to mitigate the risks whilst meeting the objectives of the processing, where possible.

A DPIA should take account of the risks to rights and freedoms of individuals and the compliance risks to Brentwood Borough Council.

The Council will be required to consider carrying out a DPIA exercise in any case where changes are proposed to:

- the purposes for which CCTV footage is used OR
- the means by which it is collected, stored or shared,

Examples of circumstances where the Council would be likely to be required to carry out a DPIA are:

- Installing new CCTV cameras to address anti social behaviour at a specific location.
- Situating cameras in location where they may overlook private properties.
- Introducing a new software system for the storage and retrieval of CCTV images.

(Please note that this is by no means an exhaustive list)

All DPIAs will be carried out in accordance with the Council's DPIA Procedure document and using the standard Council DPIA template.

The first stage of the process will be to carry out a data protection impact screening assessment exercise on the new activity to determine whether a full DPIA is required.

Where a full DPIA is deemed necessary then this must be carried out in consultation with the Data Protection Officer and signed off by the relevant business risk owner.

The DPIA will address questions such as;

- is the planned change in the use of CCTV necessary and proportionate in relation to the outcome we want to achieve?
- Will the information be processed in a safe and secure manner?
- Wil there be any impact on individuals' privacy?
- How will individuals' data protection rights be respected (such as their right to be informed about the purposes for which their information is being processed and the right to be supplied with copies of their personal information)?

The outcome of the DPIA will be to identify safeguards to reduce the risks to data subjects to a manageable and acceptable level.

If a DPIA indicates that risks are still likely to be high even after implementing safeguards it is an indication that the processing may not be appropriate and should not proceed.

If, in these circumstances, we still wish to proceed with the processing activity covered by the DPIA we will refer with the Information Commissioner's Office and ask for their approval.

All DPIAs will be kept under review in case there should be any material changes to the nature, scope, context or purposes of the activity in question.

2. STORAGE AND MANAGEMENT OF CCTV RECORDED DATA –

2.1 Brentwood Borough Council CCTV Control Room operates a Code of Practice which ensures compliance with relevant legislation in relation to the management and operation of public space CCTV.

2.2 The CCTV Control Room is staffed by vetted and SIA licensed operational staff 24 hours a day, 365 days a year. All CCTV operational staff are CRO1 and CRO2 BTEC trained. Supervisors and Management also have CRO3 BTEC training, to ensure the appropriate level of knowledge of legislation to ensure compliance with legislation for CCTV evidence data recording, monitoring, viewing and retrieval.

2.2 CCTV recordings from fixed cameras are managed and maintained in the secure CCTV Control Room, which has air locked, video access control. CCTV recording equipment is contained within an additional secure storage area within the CCTV Control Room. Access to this area is for authorised personnel by appointment only and all callers are authenticated prior to entry and required to sign in and out of the premises.

2.4 Recorded images are recorded on to stand alone Network Video Recorders and retained for 31 days before being automatically deleted. Recorded images will only be retained for longer than 31 days if a request is made under the Data Protection Act, Freedom of Information Act, the Police and Criminal Evidence Act 1984 or the Criminal Procedures and Investigations Act 1996

2.5 The system is supported by an Uninterrupted Power Supply (UPS) and generator these are programmed to maintain a power supply to essential equipment in the event of total power failure.

3. RESPONSIBLE PERSON CONTACT DETAILS

Below are the contact details of the person most qualified to respond to questions regarding this Privacy Impact Assessment.

Name:

Title:

Organisation:

Email:

Telephone:

4 CAMERA SPECIFIC - PRIOR TO INSTALLATION

Camera Location: _____

1	Why is a camera being considered for installation?				
2.	Has there been consultation before the camera was installed?	Yes		No	
2b	If yes, what was the outcome of the consultation?				
2a	If no, why wasn't it undertaken?				

5 CAMERA SPECIFIC – PRIOR TO INSTALLATION & REVIEW

3	What type of camera is being considered or in place?				
4	Is audio recording an available feature of this camera?	Yes		No	
4a	If yes; What measures are in place to protect private dialogue?				
5	Does this camera have any other camera specific or software related features such as Automatic Number Plate Recognition, Facial Recognition or Movement Analysis?	Yes		No	
5a	If yes; What software/function?				
5b	What is the purpose of having/installing this function or software?				
5c	What measures are in place to protect privacy when using this function/software?				

6	Does this camera have the capacity to record personal information as defined in paragraph 1.5?	Yes		No	
6a	If yes, please explain what and why?				
7	Is there any chance of this footage being released in the public domain?	Yes		No	
7a	If yes, explain why and what are the controls in place?				
8	Is there a Data Protection Act compliant sign clearly displayed in close proximity of the camera to make people aware that CCTV is in operation?	Yes		No	
9	Does the camera cover any part of any property where there is an expectation of privacy?	Yes		No	

9a	If yes what is covered?				
9b	What measures have been taken to prevent observation of these areas?				
10	Does any additional action need to be taken to reduce the impact on privacy by this camera?	Yes		No	
10a	If yes, please specify what action, by whom and when. (this information needs to be included in the action plan)	What: Who: When:			

6 CAMERA SPECIFIC – POST INSTALLATION REVIEW ONLY

Camera Number:

1	Has the purpose of the camera been reviewed?	Yes		No	
		Date:			
1a	What was the outcome of the Review?				
2	Has the Council ever received a complaint relating to the impact on privacy by this camera?	Yes		No	
2a	Please give details of the source and nature of the complaint and the outcome.				

Action to be taken	Responsibility of	By When	Status	Completed Date

Assessor

Signature: _____Date: _____

Print Name: _____Title: _____

Manager

Signature: _____Date: _____

Print Name: _____Title: _____

Appendix H

Surveillance Camera Commissioner

Code of Practice - A guide to the 12 principles

How well does your organisation comply with the 12 guiding principles of the surveillance camera code of practice?

Here are some questions you should consider to help you check if you comply.

1. What's your system for? Do you review its use?
2. Have you carried out a privacy impact assessment? Do you publish your privacy impact assessment?
3. Do you have signage in place to say surveillance is taking place? Is there a published point of contact for people to raise queries or complaints with?
4. Who's responsible for your system? Are your staff aware of their responsibilities?
5. Do you have clear policies and procedures in place? Do your staff know what your policies and procedures are?
6. How long do you keep images/information? How do you make sure images/information is deleted once they're no longer needed?
7. Do you have a policy on who has access to the stored information? Do you have a policy on disclosure of information?
8. Do you follow any recognised operational or technical standards?
9. Do you make sure that the images captured by your system are caught securely? Are only authorised people given access to the images?
10. Do you evaluate your system regularly to make sure it's still required? Could there be an alternative solution to a surveillance camera system?
11. Can the criminal justice system use the images and information produced by your surveillance camera system? Do you have a policy on data storage, security and deletion?
12. Do you use any specialist technology such as ANPR, facial recognition, Body Worn Video (BWV) or remotely operated vehicles (Drones)? Do you have a policy in place to ensure that the information contained on your database is accurate and up to date?

Contact the Surveillance Camera Commissioner

www.gov.uk/surveillance-camera-commissioner

Appendix I

Record of approved changes to this Code of Practice

Date	Reference	Comment	By