LONDON BOROUGH OF
RICHMOND UPON THAMES

PUBLIC SPACE
CCTV SCHEME

CODE OF PRACTICE

CODE OF PRACTICE

Introduction

The London Borough of Richmond upon Thames, Richmond upon Thames Borough of the Metropolitan Police and the local community are making progress in promoting community safety and crime prevention. The fundamental aim of this partnership is to make the Borough a safer place in which to live work and visit.

The original scheme was originally funded by the Home Office, London Borough of Richmond upon Thames and members of the London Borough of Richmond upon Thames Chamber of Commerce but since 2002 has been funded by London Borough of Richmond upon Thames.

The owner of the scheme is the Council for the London Borough or Richmond upon Thames, 44 York Street, Twickenham, Middlesex, TW1 3BZ, in partnership with Richmond upon Thames Borough of the Metropolitan Police. Both are committed to complying with this Code of Practice.

The area covered by the scheme is broken into several areas within the Borough (see Appendix A)

The system adopted includes PAL CCD high-resolution colour cameras with full pan, tilt and zoom facilities and full function dome cameras.

Each camera output will be routed to a digital recorder with real time digital recording available for specific incidents. A printer can produce hard copy prints for evidential purposes. The output of the cameras can be relayed between the Control Centre, MPS Control Rooms and the Twickenham RFU Stadium Control Room on match and event days via fibre-optic and Wi-Fi links.

The recorded material and copyright of the recorded material is in the ownership of the London Borough of Richmond upon Thames.

Purpose of Scheme

1. To discourage all types of criminal activity in the area and help reduce the fear of crime.

2. To assist the Police in providing a swift response to criminal activity and provide evidential material for court proceedings.

3. To enhance community safety, assist in developing the economic well being of the Richmond area and encourage greater use of the Town Centres, Schools and Colleges, Parks, Leisure Facilities, Shopping Centres, Car Parks, etc.

4. To promote and facilitate an active partnership in the discouragement of crime, between the Police, the Council, the Business Community and the Residents and Visitors to the Borough.

5. To assist in the compliance of Council procedure within the Borough i.e. Health & Safety Regulations.

6. To alert the emergency services in the event of fire, road traffic accidents or people needing assistance.

7. To assist in traffic management, aiding and supporting parking enforcement initiatives.

8. To assist the Local Authority in its enforcement and regulatory functions within the Borough.

9. To assist in supporting civil proceedings and internal investigations.

10. To assist in the event of a civil emergency or disaster.

The CCTV system is intended to view and monitor activity in the public spaces in the area of coverage. Every possible effort has been made in the planning and design of the CCTV system to give it maximum effectiveness but it is not possible to guarantee that the system will see every single incident taking place in the areas of coverage. The scheme is not to be used to invade the privacy of any individual in residential, business, or other private premises, buildings or land.
Signs displaying the following, or similar, wording will be installed and maintained on the camera pole and the area of coverage stating, “Images are being monitored and recorded for the purposes of public safety, crime prevention, and traffic enforcement. This scheme is controlled by the Richmond upon Thames Borough Council. For further information contact020 8891 1411”.
The Scheme makes specific arrangements for the provision of recordings for evidential purposes to the police.

Surveillance Camera Code of Practice 2013

The scheme aspires to comply with this code and particularly the 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 use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point 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.

Data Protection Act 2018 and GDPR 2018, Human Rights Act 1998, Regulation of Investigatory Powers Act 2000, Information Commissioners Office

The scheme complies, and LBRuT and its partners are committed to ensuring it complies, with all relevant legislation and guidance

Changes to the Code

Any major change will only occur after consultation with the partners of the scheme. Minor changes will be agreed by the Careline & CCTV Manager.

Responsibilities of the Owner of the Scheme

The Council for the London Borough of Richmond upon Thames, as owner, has responsibility for the compliance with the purposes and objectives of the scheme including operational guidance and the protection of the interests of the public and privacy of the individuals whose images are captured.

Management of the System

The day-to-day management of the scheme, and requirements of the Code of Practice, will be undertaken by the Careline & CCTV Manager (hereafter known as the Manager) or in that officer's absence by the Deputy Careline & CCTV Manager. All ensuing references to the Manager will be deemed to include the Deputy Careline & CCTV Manager.

Access to recordings, and the Control Room, will comply with specific guidelines and will be recorded and monitored.

The different links between the Police and the Control Room will include the ability to handover the operation of the system in the event of an incident (the level of response will be decided by the Police using the existing criteria when responding to calls for Police attendance).

The operational documentation required to run the scheme has been developed from, and is specifically linked to, the Code of Practice.

Installation

Consultation

The CCTV installations are carried out through consultation with the Police and are based on evidenced need.

Sound

No sound will be recorded in public places, however all telephone calls to the control room are recorded.

Change

Any technological change, which will have a significant effect upon the capacity of the system, will be fully assessed in relation to the purpose and key objectives of the scheme.

Dummy Cameras

No dummy cameras will be used in the scheme as they give a false sense of security and are in contravention to the DPA 2018 Code of Practice.

Accountability

Copies of the Code of Practice and complaints procedure are with each partner and can be found on the Councils internet site.

Copies of the annual report, prepared for the Community & Police Partnership group, will be made available to the public through that group

The Council will receive monthly reports on performance levels.

Police

The Police have introduced procedures to monitor and audit their participation in the scheme including compliance with the Code.

Public Information

The recording of people in public places will be undertaken fairly and lawfully. CCTV cameras will not be hidden and signs that they are operating will be displayed at the perimeter of the area of coverage. We believe that the Code of Practice should be easily available to members of the public.

The Annual Report will be prepared by the Manager and will include an evaluation of the scheme and its impact in achieving the key objectives.

Assessment of the scheme and Code of Practice

The scheme will be evaluated periodically as follows:

• The assessment of impact upon crime.

• Assessment of areas without CCTV.

• The views of the public.

• Operation of the Code of Practice.

• Whether the purposes for which the scheme was established still exist.

• Future functioning, management and operation of the scheme.

The Manager with the day-to-day responsibility for the scheme will continuously monitor the operation of the scheme and the implementation of the Code of Practice.

The Manager will undertake spot checks which will include the examination of Control Room records and the content of recorded data.

Staff

The staff employed to work in the Control Room are appointed under the council's equal opportunities fair recruitment processes. Appropriate checks will be made upon the background of individuals and will require the disclosure of relevant criminal convictions. There is a disciplinary procedure, which incorporates compliance with the Code of Practice and operational requirements and makes plain the risk to staff in the event of breaches of the Code or inappropriate handling of recordings. A requirement of confidentiality during and after termination of employment applies in staff contracts which state that staff will not during or after the period of their employment divulge to any person whatsoever, or otherwise make use of, any confidential information.

Staff will be trained in the operational skills necessary to operate a successful scheme and incompliance with the Code of Practice. Training will include how to identify suspicious behaviour, when to track individuals or groups, when to take close up views of incidents or people and compliance with RIPA, Data Protection Act and any other relevant legislation. Staff will be aware of the need not to infringe upon the publics' human rights. The effectiveness of individual operators will be reviewed.

Complaints

The Councils complaints procedure will be the vehicle for complaints. Particulars about how to make a complaint, the name and address of the person to whom the complaint should be made are publicly available in the Civic Centre.

Breaches of the Code including those of security

The Manager will investigate breaches of the Code of Practice and of security.

Control and Operation of Cameras

Information recorded will be accurate, adequate and relevant and not exceed that necessary to fulfil the purpose of the scheme.
Only staff with responsibility for using the equipment shall have access to operating controls.
Use of cameras will accord with the scheme objectives and comply with the Code of Practice.
Operators will be aware that recordings are subject to routine audit and that they may be required to justify their interest in a member of the public or premises.

Access to and Security of Monitors / Control Room

Access to view monitors, whether to operate the equipment or to view the images, is limited by the Data Protection Act 2018 to staff with that responsibility. These staff will have been trained and vetted for operations in this area.

A Control Room Access Log will record staff that are on duty each shift and the names of any persons or groups that have been authorised by the Manager to have access to the Control Room and / or view the monitors.

Public access to the Control Room shall not be allowed except by pre-arranged appointment with the manager and then only for lawful, proper and sufficient reasons. Visitors will be asked to respect the confidentiality requirements and will have to sign upon entry to the Control Room acknowledging this.

Technical repairs, cleaning and similar tasks should be carried out in controlled circumstances and people undertaking these tasks will be recorded in the access log.

Police visits to review data will be pre-arranged and appointments made. Other visits by Police must comply with the provisions of the Code of Practice and the purpose of the visit must be approved by the Manager. Access will be monitored and recorded. Occurrence and Incident Logs must be maintained on the basis of date and time throughout the day and brief details given of all incidents viewed or dealt with by operators within the Control Room, including particulars of visits and telephone calls.

Staff operating the cameras will be provided with adequate instructions on compliance with Health and Safety legislation (e.g. operating environment, lighting, position of CCTV monitors, ventilation and number of viewing hours and relationship to operator efficiency).

Recorded Material

'Recorded material' may be any media used for storing images, which can be viewed or processed after the event. It must be of good quality and be accurate in content. Security measures will be implemented to prevent unauthorised access to, alteration, disclosure or destruction, and against accidental loss or destruction of recorded material.

Statement of Intent

'Recorded material' will be used only for purposes defined in this Code of Practice.

• Access to recorded material will only take place as defined in this Code of Practice.

• Recorded material will only be accessed in accordance with the law, for investigation of crime and identification of a suspect or other lawful objective.

• Recording equipment will be checked daily to ensure it is in good working order and that the time and date generator is correctly set and displayed and certified in the daily incident log.

• DVD's required for evidential purposes will be separately indexed and securely stored and any copies handed to the Police will be sealed in an evidence bag.

Evidential use of recordings

When evidential data is downloaded onto a DVD staff will be required to provide the police with evidential statements for continuity purposes.

Police access to data

Police may apply for access, in accordance with established protocols where they reasonably believe that access to specific data is necessary for the investigation and detection of particular offence or offences or for the prevention of crime.

Police may obtain access under the provision of the Police and Criminal Evidence Act 1984.

Data provided to the Police shall at no time be used for anything other than the purpose specified when the data is released to the police by Control Room staff. The data remains, at all times, the property of the London Borough of Richmond upon Thames and shall not be disclosed to any third party, except in the lawful course of an investigation or prosecution, without the prior consent of said LBRuT.

In the circumstances described above, the Control Room will then release the data but ownership and copyright remain the Councils. The data shall at no time be used for anything other than the purpose specified and identified.

For any data to be used as evidence in any criminal proceedings there must be evidence of continuity of handling from the time it was first created in the Control Room to its production in Court as evidence.

Any evidential data released from the Control Room to the Police will be placed in an exhibit bag before leaving the Control Room. The data will be kept secure at all times thereafter and will be dealt with in accordance with current police procedures.

The data exhibited in Court, as evidence, will normally be the original recording. Working copies of the data will be provided by the Control Room staff on request.

Whilst the original data is in Police possession, working copies may be made as disclosure material to the defence.

If a person is monitoring the CCTV system when an incident occurs, the evidence of what was seen on the monitor will not be primary evidence. The person in the Control Room who causes such incident to be recorded in real time and the person who subsequently downloads data relating to such incident will be required to make statements for Court purposes.

At the conclusion of the use of any original data used by the Police, it can be retained by the police unless the Court directs that it should be destroyed.
The VTAS system will be used by LBRuT staff to record all matters relating to the disclosure of data.

Third Party Access to Data

Access to and Disclosure of Images to Third Parties

Only designated staff employed by the London Borough of Richmond upon Thames will have access and be authorised to view images on the CCTV system. This is restricted to:

• The Manager

• The Deputy Manager

• Authorised control room staff

• Other persons authorised by one of the above positions in the investigation of a particular incident or event.

These staff members are only permitted access for the purposes of carrying out their Council duties.

Appendix B will be completed where the above persons need to download or otherwise allow viewing by third parties.

Disclosure of the recorded images to third parties should only be made if disclosure is compatible with the reasons for which the CCTV cameras were installed, as detailed in the published Code of Practice.

Disclosure for these purposes must only be made to:

• Law enforcement agencies where the image(s) recorded would assist in a specific enquiry

• Prosecution agencies

• Relevant legal representatives

• The media, where it is decided that the public's assistance is needed in order to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. As part of that decision, the wishes of the victim of an incident should be considered.

• People whose images have been recorded and retained and wish to view their own images (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings) (see paragraph 7 below).

• Authorised LBRuT staff

All requests for access, or for disclosure, (other than by the police and prosecution agencies) should be made on the appropriate declaration form (Appendix B) and recorded on the relevant record sheets. Details of whether the request is accepted or denied will be documented including reasons for refusal if appropriate. In cases where access to, or disclosure of, the images is allowed, then the following is to be documented by CCTV Control Centre staff who will supervise any access to the images.

i. The date and time at which access was requested and allowed and the date on which disclosure was made
ii. The identification of any third party who was allowed access or to whom disclosure was made
iii. The reason for allowing access or disclosure
iv. The extent of the information to which access was allowed or which was disclosed.

Subject Access requests

Section 7 of the Data Protection Act 2018 and GDPR 2018 allows individuals to find out what data is held about themselves on computer and in paper records including CCTV images. This is known as the right of subject access.

Staff need to be able to recognise a request for access to recorded images by data subjects and be aware of the procedure in such circumstances. Enquiries will be referred to the senior member of CCTV control room staff on site who will initially deal with the individual who makes the request and will then contact the Manager if such a request is made.

The Data Subject will be given access to a standard subject access request form (Appendix C). This form can also be filled in by a person representing the Data Subject (for example their solicitor), where there is written authority from the Data Subject for that person to act on their behalf.

Appendix C will contain the following information:

i. The name, address and contact information of the data subject
ii. The information required in order to locate the images including all relevant dates and times and if necessary a photograph of the individual in order to locate the correct
image
iii. Indication whether the individual will be satisfied with viewing the image(s) only

Individuals will be provided with a leaflet that describes the types of images that are recorded and retained and information about the disclosure policy. This will include details of the response time the individual may expect the information to be available by and an explanation of the rights provided under the Data Protection Act 2018 and GDPR 2018.

The Council is under a legal obligation to provide access to the CCTV images. No fee is chargeable other than where requests are manifestly unfounded, excessive or repetitive when a reasonable fee will be charged based on the administrative cost of providing the information.

As part of the process the Manager will assess whether the disclosure to the individual would entail disclosing images of third parties. If it does the Manager will determine whether these images should be disclosed to the Data Subject, or whether they should be blurred or disguised. Images of other individuals should only be disclosed where:

• The other individual has consented to the disclosure; or
• It is reasonable in all the circumstances to disclose the image of the other individual without their consent. In deciding this regard shall be had for:

a) Any duty of confidentiality owed to the other individual

b) Any steps taken by the Council with a view to seeking the consent of the other individual

c) Whether the other individual is capable of giving consent (for example whether they can be located)

d) Any express refusal or consent by the other individual.

In summary, all steps should be taken to disguise or blur the features of identifiable individuals apart from the Data Subject on the CCTV image. Where it is not possible to do so, or to do so will involve significant effort, a decision must be made as to whether it is reasonable to disclose the images of the other individuals without their consent.

If the Manager decides that a subject access request from an individual is not to be complied with, the reasons for refusal should be documented on the subject access request form and a response provided**.**

The Data Subject is entitled to see his/her own images unless providing these to the Data Subject would be likely to prejudice the prevention or detection of a crime, or the
apprehension or prosecution of offenders. This must be decided on a case-by-case basis.

Other Rights/Information

An individual is entitled to serve a notice on the Council requiring the Council to cease processing images relating to that individual, or another person, on the basis that they are likely to be caused substantial, unwarranted damage or distress. All staff involved in operating the equipment must be able to recognise such a request from an individual.

The Manager is responsible for responding to such requests. Where a staff member receives a request, they must inform the Manager about this immediately.

The Manager has 21 days to respond to the request, and must indicate whether they will comply with the request or not. If the Manager decides that the request will not be complied with they will set out the reasons in the response.

Individual records should be kept referring to all the documents relating to the request and referenced for ease of access and audit purposes.

Disclosures required by law or made in connection with legal proceedings etc –
Data Protection Act 2018, Chapter 12, Section 11

Applications for data received from enquiry agents, solicitors etc will be subject to a charge dependant on the staff time required to comply but will be a minimum of £30 + VAT.

The VTAS system will be used by LBRuT staff to record all matters relating to disclosure requests.

Photographs

• Still photographs will not be taken as a matter of routine.

• Still photographs from live incidents will only be taken at the request of a police officer, who should be identified, and a record made of the request in the Incident Log, together with a note of the incident and the time and date of the request.

• A still photograph taken at a live incident, or from a recording may, be produced at the request of a police officer provided the Manager is satisfied the photograph is required for the prevention or detection of crime.

• Still photographs remain the property of the Council. A record will be kept in the Incident Log of the reason for their production, date and time, the name of the Control Room staff member responsible for producing it and will be indexed in sequence.

• Still photographs released to the police, will normally be dealt with as an exhibit.

• Still photographs will be destroyed within 28 days unless made the subject of an application from the Police or are required as evidence. A record will be kept of the destruction of all photographs in the Incident Log.

Dealing with Incidents

If during the monitoring in the Control Room, an operator sees an incident, which involves, or appears to involve, criminal activity, the operator will immediately switch to real time recording and alert the Police using the dedicated radio or telephone link or call 999 depending upon the urgency. The operator will try to obtain evidential quality footage of the event. If the police ask to take control of the camera this can be allowed but an entry must be made in the Occurrence Log.

The Control Room Operator will log the details of the incident and the communication with the Police Controller on an Incident Form (including time, date, details of what was seen and the name of the Police Officer contacted).

If, during monitoring, the operator sees an incident which does NOT appear to involve criminal activity but which may constitute a misdemeanour (traffic congestion, damage or obstruction in landscaped areas etc) the operator may alert, at the earliest opportunity, the appropriate Council officer in the relevant department whose responsibility it may be to investigate the report and take all necessary remedial action.

Again the Control Room operator will log the details of the incident and the reporting line used in the Occurrence Log.

The VTAS system will be used by LBRuT staff to record all matters relating to recorded incidents

Police Contacts and use of the System

When the Police have reasonable cause to believe that an incident has been recorded which involves, or may involve, criminal activity, a Police Officer will be permitted to view and obtain a copy of the data if it is deemed relevant.

RIPA

Any request by Police for directed CCTV surveillance of subjects or properties must be accompanied by a properly completed and authorised RIPA authorisation form 5429 **PRIOR** to surveillance commencing. If circumstances require immediate access to cameras then a copy of the completed, and authorised, RIPA form 5429 will be faxed or E Mailed to the control room **PRIOR** to the surveillance commencing.

Urgent oral authorisations, or written authorisations, granted by a person who is entitled to act only in urgent cases will, unless renewed, cease to have effect after seventy- two hours beginning at the time when the authorisation was granted or renewed

All requests for directed surveillance will be brought to the immediate attention of the Manager by control room staff.