



Southwark Council

CCTV Code of Practice

**For the use of Closed Circuit Television
(CCTV) Systems by Southwark Council.**

October 2011

1. Introduction

- 1.1 This CCTV Code of Practice governs the Council's use of CCTV to ensure:
- The Council's use of CCTV is proportionate
 - The Council meets its legal responsibilities
 - The systems are operated in line with best practice to reduce crime, anti-social behaviour, fear of crime and meet other Council priorities.
- 1.2 This CCTV Code of Practice applies to all CCTV systems operated by the Council including:
- The central public space CCTV system of 160 fixed and re-locatable cameras connected to CCTV Control Centres at Southwark Police Station and Cerise Road Car Park.
 - Re-locatable CCTV cameras operated by the Environmental Enforcement Unit (Community Safety & Enforcement Division) including vehicle mounted CCTV.
 - CCTV systems on Council Housing estates
 - CCTV in and around Council buildings such as schools, libraries and all municipal buildings.
- 1.3 All CCTV systems owned and/or operated by Southwark Council are required to comply with the minimum standards listed in appendix 1 with the exception of the request, release and management of recorded images for the purposes of parking and traffic management enforcement which are carried out in accordance with the London Councils' Code of Practice on CCTV enforcement for parking and traffic enforcement.
- 1.4 Each CCTV system is required to keep an up to date record of local information relating to purpose of the system, named responsible officers, camera use / positions, and retention of recorded images.
- 1.5 This Code of Practice also includes more in depth procedures used by the Council's central public space CCTV system for cameras connected to the CCTV monitoring suite at Southwark Police station. Other Council CCTV schemes are encouraged to adopt these procedures as best practice although some requirements will not be proportionate or appropriate for a small CCTV scheme without 24/7 live monitoring. The Council's central CCTV system also has a set of Standard Operating Procedures that provide detailed guidance to Council staff and CCTV operators.
- 1.6 The Central CCTV team adopt general responsibility for the oversight of all borough owned CCTV systems to ensure compliance with the agreed minimum standards and legislation.

2. Purpose of Southwark Council CCTV

- 2.1 The use of CCTV Systems, both fixed and temporary, will enable the Council to reduce crime, anti-social behaviour, fear of crime and to meet other Southwark Council priorities, and to support the priorities of the Safer Southwark Partnership.
- 2.2 The use of CCTV in Southwark is to:
- Deter and prevent crime;
 - Reduce the fear of crime;
 - Assist the Police, Council, and other statutory enforcement agencies in intervening in the event of crimes being committed;
 - Provide evidence relevant to the prosecution of offenders or other legal process;
 - Reduce graffiti, vandalism and other criminal damage;
 - Deter and respond to drug dealing, racial harassment and anti-social behaviour; and
 - Facilitate traffic management.

3. Definitions

- 3.1 'CCTV monitoring suite' is defined as a location where live or recorded CCTV images can be viewed, and/or where CCTV images are recorded.
- 3.2 'Independent CCTV Visitors' are defined as authorised independent volunteers undertaking visits to audit compliance with Southwark's CCTV Code of Practice. The scheme is not currently in operation; the Code of Practice will be updated once terms of reference for the scheme have been agreed.
- 3.3 'CCTV System Manager' a named individual for each system who is responsible for the operation of the system and compliance with this CCTV Code of Practice.
- 3.4 'CCTV Duty Controller' - named individual or named individuals responsible for dealing with requests to view footage on a day to day basis. This could be the same person as the CCTV System Manager if they are regularly on site.
- 3.5 'Recorded material' means any material recorded by the system including images recorded on videotape, digital formats including DVD, CD or computer integral disc, or copying onto other formats such as printed stills. All references to video tape and video recorders in this Code apply equally to digital recording media, such as Digital Audio Tape, computer discs etc.
- 3.6 Southwark Council's 'central CCTV system' is the public space system connected to the CCTV monitoring suite currently located at Borough Police station.
- 3.7 'Standard Operating Procedures' – detailed operational procedures governing the operation of the central CCTV system, particularly the CCTV monitoring suite. This is an operational document and changes can be agreed within the service by the CCTV & Coordination manager.
- 3.8 'Investigating Officer' - officers from Police, Council or other enforcement authority who is authorised to investigate reported incidents

4. Data Protection Notification

Minimum Standards

CCTV MS 1: Notification submitted to the Information Commissioner and the next renewal date recorded.

- 4.1 Note: The Council is the Data Controller for the purposes of the Data Protection Act. The Council provides an annual update to the Information Commissioner which includes use of CCTV. This is usually submitted by the Governance Team in Democratic Services. All Council CCTV Systems Managers must ensure that the purpose(s) of their CCTV system is/are included in the Council's registration with the Information Commissioner.

5. Nominated officers

Minimum Standards

CCTV MS 2: A named individual who is responsible for the operation of the system – the 'CCTV System Manager'.

CCTV MS 3: A named individual or named individuals responsible for dealing with requests to view footage on a day to day basis – 'CCTV Duty Controller'. This could be the same person as the CCTV System Manager if they are regularly on site.

6. Training

Minimum Standards

CCTV MS 4: Training will be provided to the CCTV System Manger, CCTV Duty Controller(s) and any other staff with responsibilities for the CCTV System to ensure they meet legal requirements for the operation of the system. This training can be provided by the central CCTV team upon request.

- 6.1 Note: contracted CCTV operators are legally required to be licensed by the Security Industry Authority (SIA) which includes security vetting requirements. Although not a legal requirement directly appointed staff will attend appropriate CCTV training relevant to the role.

Southwark's Central CCTV system

- 6.2 All contracted operational staff will be trained, vetted and licensed in accordance with current legislation.
- 6.3 Control Room Operational staff will receive further training on issues relevant to the London Borough of Southwark System and sign the appropriate confidentiality agreement.
- 6.4 All staff will receive training on the content of this Code of Practice and the Standard Operating Procedures manual.
- 6.5 The Council and its Contractors will ensure procedures are in place to take appropriate disciplinary action for breaches of this Code of Practice and the standard operating procedures manual, and will ensure all relevant staff are informed of the implications of such action.

7. Installation of CCTV & System choice

Minimum Standards

Prior to procurement of any new systems & upgrades design approval should be sought from the central CCTV team

CCTV MS 5: A system has been chosen that produces clear images that police, Council or other enforcement authorities can use to investigate crime and these can be easily taken from the system when required.

CCTV MS 6: Cameras are sited so that they provide clear and appropriate images.

Southwark's Central CCTV system

- 7.1 All new fixed public space CCTV cameras to be connected to the Southwark CCTV system must meet the following criteria as set out in the Southwark CCTV Strategy, agreed February 2010:
- Demonstrate how it will contribute to the priorities of Southwark Council and the Safer Southwark Partnership, supported by analysis.
 - Availability of capital and 10 year's revenue funding which does not put pressure on the councils finances.
 - Value for money
 - Meet the requirements of the Home Office Scientific Development Branch CCTV Requirements Manual 2009
 - Clear consultation process.
 - Demonstrate need for fixed cameras rather than re-locatables. (New fixed CCTV locations should first be tested by re-locatable CCTV).
- 7.2 Note: the consultation process will involve the Police and other interested parties such as community representatives and business groups.
- 7.3 Upon installation, the field of vision of each camera shall be checked and restricted to avoid any possibility of capturing views that could infringe privacy such as views into private dwellings.
- 7.4 Camera locations shall, as far as is consistent with the purposes of deployment, be in public view.

8. Signage

Minimum Standards

CCTV MS 7: There is signage showing that CCTV is in operation, with contact details and reasons for its existence.

- 8.1 Note: signage needs to be positioned at or near the perimeter of the area covered so that members of the public are aware they are entering an area of CCTV coverage.
- 8.2 Note: In exceptional and limited cases, when it is assessed that signs would not be appropriate, the Council shall ensure they have:
- (a) Identified specific criminal activity;
 - (b) Identified the need to use covert cameras to obtain evidence of that criminal activity;
 - (c) Assessed whether the use of signs would prejudice success in obtaining such evidence;
 - (d) Assessed how long the covert monitoring should take place to ensure that it is not carried out for longer than is necessary; and
 - (e) Documented (a) to (d) above.
- 8.3 Note: The provisions of the Regulation of Investigatory Powers Act (RIPA) 2000 will need to be considered when covert surveillance is anticipated. See section 16.

9. Recording of, and access to, images

Minimum Standards

- CCTV MS 8: Images from the CCTV system are securely stored, where only a limited number of authorised persons may have access to them.
- CCTV MS 9: Recorded images will only be retained for long enough for an incident to come to light and relevant footage reviewed. Recorded images will not normally be retained for more than 31 days, and there must be procedures in place to wipe or overwrite unless required as evidence.
- CCTV MS 10: Recorded images can only be viewed by officers from Police, Council or other enforcement authority assigned to investigate reported incidents once they have satisfied the 'CCTV Duty Controller' Data Handler/Controller that their request falls within the principles of this Code of Practice.

- 9.1 Note: This includes requests for video stills.
- 9.2 Note: If footage is released to an Investigating Officer, the Investigating Officer is required to sign a disclaimer to confirm they take responsibility for all aspects of the footage including safekeeping, secure storage, further disclosure, continuity, integrity and final destruction in line with the Data Protection Act, and that in all instances where the Investigating Officer is a non-council officer, responsibility will transfer to that officer's organisation as Data Controller'.

Southwark's Central CCTV system

- 9.3 Council Departments may have access in respect of the proper transaction of Council business, through requests from the appropriate manager to the Central CCTV management team who will assess if the request is proportionate.
- 9.4 Access may also be gained by application through the Court.
- 9.5 In all cases, reviewing shall be carried out under the supervision of the CCTV Duty Controller.

Procedures for Investigating Officers

- 9.6 When an Investigating Officer has reasonable cause to believe that an incident may have been recorded, they will contact the Control Room or CCTV systems manager/duty officer to agree an appointed time to attend the system to review possible evidence. Investigating officers are required to give reasons in writing, including all statutory provisions relied on, for requesting to view footage as part of the standard control room documentation.
- 9.7 Reviews will be carried out in accordance with current legislation as detailed in the Standard Operating Procedures Manual.
- 9.8 The Council and their Contractors will provide witness statements where appropriate and all release documentation will be completed before any data is released from the Control Centre.

Use of Tapes

- 9.9 A log will be maintained to log the use of all tapes.
- 9.10 Prior to recording, the equipment and the tapes will be checked to ensure all is in good working order.
- 9.11 The time and date generator shall be checked to ensure it is correctly set.

10. Dealing with Incidents

Minimum Standards

CCTV MS 11: Procedures are in place to respond to an incident recorded on the system, e.g. the Duty Controller will dial 999 in the event of an emergency.

- 10.1 The Standard Operating Procedures manual sets out how CCTV operators will deal with incidents.

11. Subject Access Requests and Freedom of Information Requests

Minimum Standards

CCTV MS 12: Procedures are in place to respond to Subject Access Requests (requests under the Data Protection Act for individuals requesting copies of their own images) and Freedom of Information requests.

- 11.1 Procedures for Subject Access Requests are detailed in the Standard Operational Procedures Manual and the subject access request form is available on the Council's website.
- 11.2 The CCTV System Manager will ensure all subject access requests are dealt with within 40 calendar days of their receipt and in accordance with the standards defined in the CCTV Codes of Practice published by the Information Commissioner and in sections 7, 10, 12 and 13 of the Data Protection Act, 1998.
- 11.3 Freedom of Information requests will be dealt with promptly and within 20 working days of their receipt.
- 11.4 The CCTV System Manager will ensure all subject access and freedom of information requests and the responses are recorded, and notify the Council's Corporate Freedom of Information Officer.
- 11.5 The CCTV System Manager is entitled to withhold personal data from an individual making a subject access request, where it is considered that to disclose the personal data would be likely to prejudice either:
 - (a) Prevention or detection of crime, or
 - (b) Apprehension or prosecution of offenders.

12. Administration and record keeping

Minimum Standards

CCTV MS 13: An administration system will be in place to log: incidents and responses to incidents, requests to view recorded images, copies of recorded images released, Subject Access Requests and Freedom of Information requests. For a small system this may be a single record sheet covering everything.

CCTV MS 14: All requests to view footage must be signed by the investigating officer, and the decision (refusal or authorisation), signed by the CCTV Duty Controller.

CCTV MS 15: All recorded footage released to investigating officers must be signed for by the investigating officer and the CCTV Duty Controller.

13. Annual Review

Minimum Standards

CCTV MS 16: The use of the CCTV system, and compliance with the above minimum standards, will be reviewed annually.

Central CCTV system

- 13.1 The CCTV & Coordination Manager will produce an annual report detailing performance of the CCTV system against its objectives, technical performance, Subject Access Requests, deployments of relocatable cameras, details of any evaluations. The annual report will be published on the Council's website and circulated to Safer Southwark Partnership members.
- 13.2 All systems managers will compile an individual report pertinent to their system for inclusion in the annual report.

14. System Management

Minimum Standards

CCTV MS 17: Regular checks are carried out to ensure that the system is working properly and produces high quality images.

- 14.1 Note: Appropriate repairs and maintenance arrangements must be in place to address identified issues to ensure compliance with CCTV MS 5 and 6.

15. Management of Control Rooms

Southwark Police Station and Cerise Road Car Park Control Rooms

- 15.1 The Control Room at Southwark Police Station will be staffed at all times with a minimum of one Operator actively monitoring the equipment, except for the purpose of emergency evacuation. In which case, procedures for such evacuation, detailed in the Standard Operating Procedures will be followed.
- 15.2 The Control Room at Cerise Road will be staffed only during hours of enforcement of parking and other road traffic offences, except in case of emergency cover in the event of evacuation or equipment failure at the control room at Southwark Police Station.
- 15.3 All visitors to both Control Rooms will be recorded in a log maintained for that purpose.
- 15.4 Access to the Control Rooms shall be regulated by the CCTV System Manager or person(s) authorised to do so.
- 15.5 Access shall be given to:
 - (a) Operatives employed by the Council or its Contractor for the purpose of managing, operating and maintaining the System.
 - (b) Council, Police and other Investigating Officers authorised to do so.
 - (c) Independent CCTV Visitors.

16. Regulation of Investigatory Powers Act (RIPA)

- 16.1 The Council (and those working on its behalf) has a duty to ensure it does so in a way which is compatible with the Human Rights Act 1998 (HRA), which protects the private and family life of citizens. The use of overt CCTV cameras which are permanently sited for the purposes of e.g. monitoring traffic flow or public safety will not generally be incompatible with the HRA because the public will be aware that such systems are in use – ie the cameras will be readily visible and there will be prominently displayed signs stating that CCTV surveillance is in operation. Such surveillance is generally overt.
- 16.2 If the Council wishes to use such a camera for a specific investigation or operation, or to monitor the activities of a particular person or group of individuals, then that surveillance is both directed (ie targeted) and is covert, in that the individuals in question will not be aware that they are being specifically targeted. In these circumstances the Council must comply with the Regulation of

Investigatory Powers Act 2000 (RIPA), which provides a mechanism for authorising directed covert surveillance which would otherwise be incompatible with the HRA.

- 16.3 A RIPA authorisation can only be granted by an Authorising Officer in writing (except in an emergency) and can only be obtained for the purpose of the prevention or detection of crime or the prevention of disorder. The Authorising Officer must be satisfied that the proposed use of the CCTV camera is both necessary and proportionate to desired outcome, having particular regard to the gravity and extent of the activity under investigation.
- 16.4 Further details, including a list of Authorising Officers, can be found in the Council's Policy & Procedures on Covert Surveillance and the Home Office Code of Practice on the RIPA site on The Source. If in doubt as to the application of RIPA, legal advice should always be sought before commencing surveillance.
- 16.5 Investigating officers wishing to use the Council's CCTV systems for directed covert surveillance images are responsible for obtaining appropriate RIPA authorisations from within their organisation.
- 16.6 Investigating officers must provide details of their RIPA authorisation to the CCTV Duty Controller. The CCTV Duty Controller will refuse requests if details of the RIPA authorisation are not provided.
- 16.7 Details of RIPA authorisations for use of the Council's CCTV systems for directed covert surveillance will be passed by the CCTV Duty Controller to be recorded on the Council's central RIPA register.

17. Provision for Special Contingencies

Council's Central CCTV System

- 17.1 In the event or prospect of serious disorder or other major incident, the Chief Executive (or officer nominated by the Chief Executive) may authorise the Police to enter and manage a Control Room.
- 17.2 Control Room staff will remain in attendance to assist in the operation of the equipment. In severe or extremely sensitive cases, CCTV Operators may be requested to leave the premises, handing complete control to the Police. Details of such incidents and procedures are set out in the Standard Operating Procedures Manual.

18. Media Disclosure

- 18.1 All media requests for footage from Council CCTV systems will be referred to the Council's Communications team.
- 18.2 The release of footage for media purposes must be authorised by the Head of Communications and the Head of Community Safety & Enforcement.
- 18.3 Personal data will be removed, including third parties, witnesses and victims unless the Head of Community Safety & Enforcement and the Head of Communications have agreed the release of personal data will contribute to meeting the objectives of the CCTV system or for the transaction of other Council business.
- 18.4 The release of footage must be accompanied by a release document signed by the Council and the media organisation that clearly states what the footage will be used for and sets out the limits on its use including how long the footage can be retained once it is released.
- 18.5 The release form shall state that the receiver must process the data in a manner prescribed by the data controller, e.g. specific identities/data that must not be revealed.
- 18.6 The release form shall be considered a contract and signed by both parties.

19. Accountability

- 19.1 Any perceived breaches of this Code shall be reported to the CCTV System Manager to investigate. If the person reporting the breach is unsatisfied with the response, they should report it to the CCTV & Coordination manager for further investigation.

Council's Central CCTV System

- 19.2 The supervision and management of the Control Rooms will be monitored by Independent CCTV Visitors, to ensure that this Code of Practice is complied with. Access by its members shall not be unreasonably denied by the Council or its contractors, unless the integrity of any recorded evidence may be compromised.
- 19.3 In the event of a serious breach of this Code, either the Council or the Police complaints and disciplinary procedures will be adopted, or those of a Contractor, depending on the nature of the alleged breach and the person(s) who have been alleged to have committed the breach.
- 19.4 The Independent CCTV Visitors will meet at Bi annually with Council and Police representatives to review CCTV operations and will submit an annual report to the Southwark Police Consultative Group.
- 19.5 Copies of this Code of Practice will be available on the Council's website.
- 19.6 Complaints relating to the use of any CCTV System within the control of the London Borough of Southwark should be made through the Council's complaints procedure. Details are available on the Council's website.
- 19.7 Complaints from staff employed by Council contractors about the contractor's internal management or other human resources issues should be referred to the contractor as their employer to be dealt with in line with the contractor's complaints and HR procedures.
- 19.8 Complaints from staff employed by Council contractors about Southwark Council staff should either be raised with the management of the contractors for them to raise at routine contract monitoring meetings with Southwark Council or, to use the Council's complaints procedure. Details of the Council's complaints procedure are available on the Council's website.
- 19.9 The Council's contractors are required to comply with this Code of Practice and persistent and/or serious breaches will be dealt with via contract monitoring procedures and could result in penalties or termination of the contract.
- 19.10 The central CCTV team will conduct periodic audits of systems to ensure the Code of Practice is being complied with.

20. Review of this Code of Practice

- 20.1 This Code of Practice will be reviewed annually and the findings reported to Independent CCTV Visitors.
- 20.2 Amendments to this Code of Practice shall be agreed by the Head of Community Safety & Enforcement in consultation with the Chief Supt Partnership.
- 20.3 The Independent CCTV Visitors will be consulted on changes to the Code of Practice.

21. More Information

21.1 Further information can be obtained from:

The Southwark CCTV strategy <http://moderngov.southwarksites.com/mgConvert2PDF.aspx?ID=7784>

The Information Commissioner's website www.ico.gov.uk

Southwark Council's website www.southwark.gov.uk

Minimum Standards for Southwark Council CCTV Systems

1. Notification submitted to the Information Commissioner and the next renewal date recorded.
2. A named individual who is responsible for the operation of the system – the ‘CCTV System Manager’.
3. A named individual or named individuals responsible for dealing with requests to view footage on a day to day basis – ‘CCTV Duty Controller’. This could be the same person as the CCTV System Manager if they are regularly on site.
4. Training will be provided to the CCTV System Manager, CCTV Duty Controller(s) and any other staff with responsibilities for the CCTV System to ensure they meet legal requirements for the operation of the system.
5. A system has been chosen that produces clear images that police, Council or other enforcement authorities can use to investigate crime and these can be easily taken from the system when required.
6. Cameras are sited so that they provide clear and appropriate images.
7. There is signage showing that CCTV is in operation, with contact details and reasons for its existence.
8. Images from the CCTV system are securely stored, where only a limited number of authorised persons may have access to them.
9. Recorded images will only be retained for long enough for an incident to come to light and relevant footage reviewed. Recorded images will not normally be retained for more than 31 days, and there must be procedures in place to wipe or overwrite unless required as evidence.
10. Recorded images can only be viewed by officers from Police, Council or other enforcement authority assigned to investigate reported incidents once they have satisfied the ‘CCTV Duty Controller’ Data Handler/Controller that their request falls within the principles of this Code of Practice.
11. Procedures are in place to respond to an incident recorded on the system, eg the Duty Controller will dial 999 in the event of an emergency.
12. Procedures are in place to respond to Subject Access Requests (requests under the Data Protection Act for individuals requesting copies of their own images) and Freedom of Information requests.
13. An administration system will be in place to log: incidents and responses to incidents, requests to view recorded images, copies of recorded images released, Subject Access Requests and Freedom of Information requests. For a small system this may be a single record sheet covering everything.
14. All requests to view footage must be signed by the investigating officer, and the decision (refusal or authorisation), signed by the CCTV Duty Controller.
15. All recorded footage released to investigating officers must be signed for by the investigating officer and the CCTV Duty Controller.
16. The use of the CCTV system, and compliance with the above minimum standards, will be reviewed annually.
17. Regular checks are carried out to ensure that the system is working properly and produces high quality images.