ROYAL borough of GREENWICH

Code of Practice for the operation of the Community Safety Closed Circuit Television System

in partnership with

METROPOLITAN POLICE Working for a safer London

September 2018
Version 10.0

Code of Practice in respect of the operation of the Royal Borough of Greenwich Borough Community Safety CCTV System

Agreed by

Royal Borough of Greenwich
and
Metropolitan Police Service

Certificate of Agreement

The content of both this Code of Practice and the Procedural Manual are hereby approved in respect of the Royal Borough of Greenwich Borough Community Safety 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 Community Safety CCTV System.

Signed for and on behalf of Royal Borough of Greenwich

Signature: .....

Name: ..... Position held: .....

Dated the ..... day of ..... (month) ..... (year)

Signed for and on behalf of Metropolitan Police Service

Signature: .....

Name: ..... Position held: .....

Dated the ..... day of ..... (month) ..... (year)

Document Control

Distribution:

Name	Job Title
Corporate Data Guardian	Corporate Data Guardian Customer Services & ICT Strategy
Lorraine Hancock	CCTV System Assistant Manager Directorate of Housing & Safer Communities
Dave Downs	Manager Street Wardens, Trading Standards and CCTV Directorate of Housing & Safer Communities
Ray Seabrook	Assistant Director Directorate of Housing & Safer Communities

Change History:

Version	Issued	Reason for Change	Issued By
1.0	November 2004	Draft created	Graeme James
2.0	May 2005	Final Draft for Comment	Graeme James
3.0	May 2006	Amended final draft incorporating comments	Keith Archard
4.0	November 2009	Updated camera list and contacts	Keith Archard
5.0	December 2012	Upgrade and modernisation of control room	Keith Archard
6.0	November 2013	Updated camera list appendix G	Keith Archard
7.0	March 2014	Contact name amendment	Keith Archard
8.0	March 2015	Updated to reflect new Home Office guidance	Keith Archard
9.0	November 2017	Update to reflect changes to camera list and staff changes	Lorraine Hancock
10.0	September 2018	Update to reflect changes to the Data Protection Act and General Data Protection Regulations	Lorraine Hancock

Contents

1. Introduction and Objective

1.1. Introduction

1.1.1. A Closed Circuit Television (CCTV) system exists within the Royal Borough of Greenwich. This system, known as the Community Safety CCTV system, comprises of a number of cameras installed at strategic locations within town centres, car parks, open spaces, housing estates, foot tunnels and other public areas. Many cameras have pan, tilt and zoom facilities and other cameras are in fixed positions. The images are presented in the CCTV control room where they are monitored and recorded. Limited secondary monitoring takes place at a nominated alternative Police location but there are no recording or control facilities at this location.

1.1.2. The Directorate of Housing & Safer Communities CCTV System has evolved from the formation of a Community Safety Partnership between:

- Royal Borough of Greenwich
- Metropolitan Police Service
- National Probation Trust
- London Community Rehabilitation Company
- London Fire Brigade
- NHS Greenwich Clinical Commissioning Group

Assisted by:

- Woolwich Development Agency
- Greenwich Development Agency
- South Greenwich Development Agency

1.1.3. For the purposes of this document, 'the System' refers to the Directorate of Housing & Safer Communities CCTV System.

1.1.4. For the purposes of this document, 'the Owner' of The System is the Royal Borough of Greenwich.

1.1.5. For the purposes of the Data Protection Act 2018 and GDPR 2018, 'The Data Controller' is the Royal Borough of Greenwich.

1.1.6. The officer named as 'the System Manager' is Dave Downs.

1.1.7. The officer with responsibilities for the Data Protection Act 2018 and GDPR 2018 is the RBG Data Guardian.

1.1.8. The Royal Borough CCTV system has been notified to the Information Commissioner.

1.1.9. Details of key personnel, their responsibilities and contact points are shown at appendix A to this Code of Practice (hereafter referred to as 'this Code').

1.1.10. This document will be reviewed annually in order to take into account changes to procedure or legislation.

1.2. Partnership Statement in Respect of The Human Rights Act 1998 (Article 8)

1.2.1. The partnership recognises that public authorities and those organisations carrying out the functions of a public service nature are required to observe the obligations imposed by the Human Rights Act 1998, and consider that the use of CCTV in the Royal Borough of Greenwich is a necessary, proportionate and suitable tool to help reduce crime, reduce the fear of crime and improve public safety.

1.2.2. Section 163 of the Criminal Justice and Public Order Act 1994 creates the power for local authorities to provide closed circuit television coverage of any land within their area for the purposes of crime prevention and detection and it is also considered a necessary initiative by the Partners towards their duty under the Crime and Disorder Act 1998.

1.2.3. It is recognised that operation of the System may be considered to infringe on the privacy of individuals. The partnership recognises that it is their responsibility to ensure that the System should always comply with all relevant legislation, to ensure its legality and legitimacy. The System will only be used as a proportional response to identified problems and be used only in so far as it is necessary in a democratic society, in the interests of national security, public safety, the economic well-being of the area, for the prevention and detection of crime or disorder or for the protection of the rights and freedoms of others.

1.2.4. This Code and observance of the Operational Procedures contained in the manual shall ensure that evidence is secured, retained and made available as required to ensure there is respect for everyone's right within law to a free trial.

1.2.5. The System shall be operated with due regard for the need to eliminate unlawful discrimination harassment and victimisation and other conduct prohibited by the Equality Act 2010

1.3. Objectives of the System

1.3.1. The objectives of the System as determined by the owners / partnership which form the lawful basis for the processing of data are:

- To reduce the fear of crime, disorder and anti-social behaviour.
- To deter crime.
- To detect crime and provide evidential material for court proceedings.
- To enhance community safety, assist in developing the economic well-being of the Royal Borough of Greenwich and encourage greater use of the town centres, university, car parks, open spaces and shopping areas etc.
- To assist the Local Authority in its enforcement and regulatory functions within the Royal Borough of Greenwich.
- To assist in Traffic Management.
- To assist in supporting civil proceedings, which will help detect crime.
- Any other specific objective identified by the owners or partners of the scheme.

1.4. Procedural Manual

1.4.1. This Code is supplemented by a separate 'Procedural Manual', which gives instructions on aspects of the day-to-day operation of the system. To ensure the purpose and principles (see Section 2) of the System are realised, the procedural manual is based and expands upon the contents of this Code.

2. Statement of Purpose and Principles

2.1. Purpose

2.1.1. The purpose of this document is to state the intentions of the system owners and managers, on behalf of the partnership, to support the objectives of the System, and to outline how it is intended to do

2.1.2. The purpose of the System, and the process adopted in determining the reasons for implementing the System have been defined in order to achieve the objectives detailed within Section 1.

2.2. General Principles of Operation

2.2.1. The system will be operated in accordance with all the requirements and the principles of the Human Rights Act 1998.

2.2.2. The operation of the system will also recognise the need for formal authorisation of any covert 'Directed' surveillance or crime trend (hotspot) surveillance as required by the Regulation of Investigatory Powers Act 2000.

2.2.3. The System will be operated in accordance with the Data Protection Act 2018 and GDPR 2018 at all times.

2.2.4. The System will be operated with due regard to the guidelines set out within Surveillance Camera Commissioners Code of Practice 2013.

2.2.5. The System will be operated fairly, within the law, and only for the objectives for which it was established and are identified within this Code, or which are subsequently agreed in accordance with this Code.

2.2.6. The public interest in the operation of the system will be recognised by ensuring the security and integrity of operational procedures.

2.2.7. Throughout this Code it is intended, as far as reasonably possible, to balance the objectives of the System with the need to safeguard the individual's rights. Every effort has been made throughout this Code to indicate that a formal structure has been put in place, including a complaints procedure, by which it can be identified that the management of the System is not only accountable, but is seen to be accountable.

2.2.8. Participation in the system by any organisation, individual or authority assumes an agreement by all such participants to comply fully with this Code and to be accountable under this Code.

2.3. Copyright

2.3.1. Copyright and ownership of all material recorded by virtue of the System will remain with the data controller.

2.4. Cameras and Area Coverage

2.4.1. The areas covered by CCTV to which this Code refers are the public areas within the responsibility of the operating partners as listed below.

- A total of 208 PTZ (pan-tilt-zoom) on-street cameras in the following areas:
  - Barnfield Estate (5)
  - Cardwell Estate (10)
  - East Greenwich (8)
  - Eltham Town Centre (7)
  - Eynsham Drive / Abbey Wood (4)
  - Glyndon Estate (25)
  - Greenwich Riverside Walk (17)
  - Greenwich Town Centre (27)
  - Plumstead High Street / Sewerbank (24)
  - Polthorne Estate (5)
  - Roads surrounding Queen Elizabeth Hospital (3)
  - Eltham / Horn Park Estate (9)
  - Well Hall / Pleasance (13)
  - Woolwich Common Estate (3)
  - Woolwich Dockyard (7)
  - Woolwich Town Centre (41)
  - St Georges Chapel (3)

- A total of 52 fixed cameras in the following foot tunnels:
  - Woolwich (26)
  - Greenwich (26)
- A total of 461 fixed cameras in the following housing estates:
  - Cardwell Estate (200)
  - Glyndon Estate (131)
  - Woolwich Common Estate (130)
  - A Grand total of 724 cameras

2.4.2. From time to time transportable or mobile cameras may be temporarily sited within the area. The use of such cameras, and the data produced by virtue of their use, will always accord with the objectives of the System and be governed by this Code and the Procedural Manual.

2.4.3. Many of the cameras offer full colour, pan tilt and zoom (PTZ) capability, some of which may automatically switch to monochrome in low light conditions.

2.4.4. None of the cameras forming part of the System will be installed in a covert manner. Some cameras may be enclosed within 'all weather domes' for aesthetic or operational reasons but the presence of all cameras will be identified by appropriate signs.

2.4.5. An annual review of all cameras will take place to ensure that they continue to meet the stated objectives of the System and there is consideration made to the Privacy Impact.

2.5. Monitoring and Recording Facilities

2.5.1. The CCTV equipment has the capability of recording all cameras simultaneously throughout every 24 hour period.

2.5.2. No equipment, other than that housed within the main CCTV control room shall be capable of recording images from any of the cameras.

2.5.3. All images are recorded onto digital video recorders. All viewing and recording equipment shall only be operated by trained and authorised users.

2.6. Processing and Handling of Recorded Material

2.6.1. All digitally recorded material will be processed and handled strictly in accordance with this Code and the Procedural Manual.

2.7. Operators Instructions

2.7.1. Technical instructions on the use of equipment housed within the monitoring room are contained in a separate manual provided by the equipment suppliers.

2.8. Changes to the Code of Practice or the Procedure Manual

2.8.1. Any major changes to either this Code or the Procedural Manual, (i.e. something that will have a significant impact upon this Code or upon the operation of the system) will take place only after consultation with, and upon the agreement of the Safer Greenwich Partnership.

2.8.2. A minor change, (i.e. such as may be required for clarification and will not have such a significant impact) may be agreed between the manager and the owners of the System and this will be documented and dated.

3. Privacy and Data Protection

3.1. Public Concern

3.1.1. 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.

3.1.2. All personal data obtained by virtue of the 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 due regard for everyone's right to respect for his or her private and family life and their home.

3.1.3. The storage and security of the data will be strictly in accordance with the requirements of the Data Protection Act 1998.

3.2. Data Protection Legislation

3.2.1. The operation of the System has been notified to the Office of the Information Commissioner in accordance with current Data Protection legislation.

3.2.2. The Data Controller for the System is the Royal Borough of Greenwich and day to day responsibility for the data will be devolved to the System Manager.

3.2.3. All data will be processed in accordance with the principles of the Data Protection Act, 2018 and GDPR which, in summarised form, includes, but is not limited to:

I. Data shall be processed fairly and lawfully.
II. Data shall be obtained/processed for specific lawful purposes.
III. Data held must be adequate, relevant and not excessive.
IV. Data must be accurate and kept up to date.
V. Data shall not be kept for longer than necessary.
VI. Data shall be processed in accordance with rights of data subjects.
VII. Data must be kept secure.
VIII. Data shall not be transferred outside the EEA unless there is adequate protection.

3.3. Requests for Information

3.3.1. Any request from an individual for the disclosure of personal data which they believe is recorded by virtue of the System will be directed in the first instance to the officer responsible for data protection.

3.3.2. The principles of Sections 7 and 8, of the Data Protection Act 2018 shall be followed in respect of every request; those Sections are reproduced as Appendix B to this Code.

3.3.3. If the request cannot be complied with without identifying another individual, permission from all parties must be considered (in the context of the degree of privacy they could reasonably anticipate from being in that location at that time) in accordance with the requirements of the legislation.

3.3.4. 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 appropriate 'Subject Access' request form is included in Appendix F.

3.4. Individual Subject Access Under Data Protection Legislation

3.4.1. 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 fee of £10.00 is paid in advance for each individual search.
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.

3.4.2. In the event of the data controller complying with a request to supply a copy of the data to the subject, only data pertaining to the individual should be copied, (all other personal data which may facilitate the identification of any other person should be concealed or erased). Under these circumstances an additional fee may be payable and will vary dependant on the extent of the concealment required.

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

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

I. The original data and that the audit trail has been maintained.
II. Not removed or copied without proper authority.
III. For individual disclosure only (i.e. to be disclosed to a named subject).

3.5. Process of Disclosure

3.5.1. Set procedures for disclosure be followed:

I. Verify the accuracy of the request.
II. Replay the data to the requestor only, (or responsible person acting on behalf of the person making the request).
III. The viewing should take place in a separate room and not in the CCTV control room. Only data which is specific to the search request shall be shown.
IV. 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).
V. If a copy of the material is requested and there is no on-site means of editing out other personal data, then the material shall be sent to an editing house for processing prior to being sent to the requestor.

3.6. Media Disclosure

3.6.1. All requests from the media for access to recorded material will be directed to the Royal Borough of Greenwich's Communications Section who will seek a decision to release the data.

3.6.2. If the means of editing out other personal data does not exist on-site, the following procedures shall be adopted:

I. In this event the following procedures shall be adopted:
II. 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.
III. 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.
IV. It shall require that proof of any 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 the System's Code of Practice).
V. The release form shall be considered a contract and signed by both parties

3.7. Exemptions to the Provision of Information

3.7.1. In considering a request made under the provisions of Section 7 of the Data Protection Act 2018 and GDPR, reference may also be made to Section 29 of the Act which includes, but is not limited to, the following statement:

Personal data processed for any of the following purposes -

I. the prevention or detection of crime
II. the apprehension or prosecution of offenders

are exempt from the subject access provisions in any case to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection.

3.8. Criminal Procedures and Investigations Act 1996

3.8.1. The Criminal Procedures and Investigations Act, 1996 came into effect in April 1997 and introduced a statutory framework for the disclosure to defendants of material, which the prosecution would not intend to use in the presentation of its own case, (known as unused material). Disclosure of unused material under the provisions of this Act should not be confused with the obligations placed on the data controller by Section 7 of the Data Protection Act 1998.

4. Accountability and Public Information

4.1. The Public

4.1.1. For reasons of security and confidentiality, access to the CCTV monitoring room is restricted in accordance with this Code.

4.1.2. 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 in order to ensure 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 and monitored for compliance via spot checks.

4.1.3. A member of the public wishing to register a complaint with regard to any aspect of the System may do so by contacting the System Manager's office. All complaints shall be dealt with in accordance with the Royal Borough of Greenwich's complaints procedure, a copy of which may be obtained from any Royal Borough of Greenwich office or via the website. Any performance issues identified may be considered under the organisations disciplinary procedures to which all personnel of the Royal Borough of Greenwich are subject.

4.1.4. All CCTV staff are contractually subject to regulations governing confidentiality and discipline. An individual who suffers damage or distress by reason of any contravention of this Code may be entitled to compensation.

4.2. System Owner

4.2.1. The System Owner will have unrestricted personal access to the CCTV monitoring room and will be responsible for receiving as required regular and frequent reports from the System Manager.

4.2.2. The Royal Borough of Greenwich will report to the Safer Greenwich Partnership which will have a specific responsibility for receiving and considering those reports.

4.2.3. Formal consultation will take place between the owners and the managers of the system with regard to all aspects, including this Code and the Procedural Manual.

4.3. System Manager

4.3.1. The nominated manager named at Appendix A will have day-to-day responsibility for the System as a whole.

4.3.2. The System will be subject to compliance auditing by the Royal Borough of Greenwich's Head of Governance, Systems Performance and Customer Experience Customer Services and ICT Strategy or nominated deputy.

4.3.3. The System Manager will respond to complaint, in writing, within fifteen working days, including advice to the complainant of the enquiry procedure to be undertaken. A formal report will be forwarded to the system owner or their nominee, giving detail of all complaints and the outcome of relevant enquiries.

4.3.4. Statistical and other relevant information, including any complaints made, will as appropriate be included in the Annual Reports of the Royal Borough of Greenwich, which are made publicly available.

4.4. Public Information

4.4.1. The following information shall be published on the Royal Borough of Greenwich web site, and a copy will be made available to anyone on request:

- Code of Practice
- Annual Review
- Service Standards
- Annual Performance Report
- CCTV Operational Strategy

4.5. Signs

4.5.1. Signs (As Shown below) will be placed in the locality of the cameras and at main entrance points to the relevant areas. The signs will indicate:

I. The presence of CCTV monitoring.
II. The 'ownership' of the system.
III. Contact telephone number of the 'data controller' of the system.

5. Assessment of the System and Code of Practice

5.1. Annual Review

5.1.1. The System will be reviewed annually to establish whether the purposes of the system are being complied with and whether objectives are being achieved. The review will cover compliance with:

I. Operational Requirements
II. Privacy Impact Assessment
III. Service Standards
IV. Surveillance Commissioners Code of Practice

5.1.2. The results of the review will be published and will be used to review and develop any alterations to the specified purpose and objectives of the scheme as well as the functioning, management and operation of the System.

5.2. Monitoring

5.2.1. The System Manager will accept day to day responsibility for the monitoring, operation and evaluation of the system and the implementation of this Code.

5.2.2. The System Manager shall also be responsible for maintaining full management information as to the data produced by the CCTV operators, for use in the management of the System and in reviews.

5.3. Inspection

5.3.1. Lay inspectors who have no direct contact or relationship with the operation of the System may be appointed by the System Owner to be responsible for inspecting the operation of the System.

5.3.2. Inspections should take place annually by no more than two people. The inspectors will be permitted access to the CCTV control room, without prior notice and to the records held therein, provided their presence does not disrupt the operational functioning of the service. Their findings will be reported to the System Owner and their visit recorded in the CCTV control room access log.

5.3.3. Inspectors will be required to sign a declaration of confidentiality (see Appendix E).

6. Human Resources

6.1. Staffing of the CCTV Control Room and Those Responsible for the Operation of the System

6.1.1. The CCTV Control Room will be staffed in accordance with the procedural manual. Equipment associated with The System will only be operated by authorised personnel who will have been properly trained in its use and all monitoring room procedures.

6.1.2. Every person involved in the management and operation of the System will be issued with a personal copy of both this Code and the Procedural 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. 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.

6.1.3. All personnel involved with the System shall receive training in respect of all legislation appropriate to their role.

6.1.4. All staff will be subject to non-police personnel vetting procedures.

6.2. Discipline

6.2.1. Every individual with responsibilities under the terms of this Code and who has any involvement with the System to which they refer, will be subject to the Royal Greenwich disciplinary procedures. Any breach of this Code or of any aspect of confidentiality will be dealt with in accordance with those discipline rules.

6.2.2. The System Manager will accept primary responsibility for ensuring there is no breach of security and that this Code is complied with. They have day-to-day responsibility for the management of the control room and for enforcing the discipline rules.

6.3. Declaration of Confidentiality

6.3.1. Every individual with responsibilities under the terms of this Code and who has any involvement with the System to which they refer, will be required to sign a declaration of confidentiality. (See example at appendix D; see also Section 8 concerning access to the monitoring room by others).

7. Control and Operation of Cameras

7.1. Guiding Principles

7.1.1. Any appropriately authorised and trained person operating the cameras will act with utmost probity at all times.

7.1.2. The cameras, control equipment, recording and reviewing equipment may only be operated by persons who have been trained in their use and the legislative implications of their use.

7.1.3. Every use of the cameras will accord with the purposes and objectives of the system and shall be in compliance with this Code.

7.1.4. Camera operators will be mindful of exercising prejudices that 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 system manager.

7.2. Operation of the System by the Police

7.2.1. Under certain circumstances the Police may make a request to assume direction of the System to which this Code applies. Only requests made on the written authority of a police officer not below the rank of Inspector 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.

7.2.2. In the event of such a request being permitted, the Monitoring Room will continue to be staffed, and equipment operated by, only those personnel who are authorised to do so, and who fall within the terms of Sections 6 and 7 of this Code, who will then operate under the direction of the police officer designated in the written authority.

7.2.3. In very extreme circumstances a request may be made for the Police to take total control of the System in its entirety, including the staffing of the monitoring room and personal control of all associated equipment, to the exclusion of all representatives of the System Owners. Any such request should be made to the System Manager in the first instance, who will consult personally with the most senior officer of the System 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 person of equal standing.

7.3. Maintenance of the System

7.3.1. To ensure compliance with the Information Commissioners Code of Practice and that images recorded continue to be of appropriate evidential quality the System shall be maintained in accordance with the requirements of the Procedural Manual under a maintenance agreement.

7.3.2. The maintenance agreement will make provision for regular/ periodic service checks on the equipment which will include cleaning of any all-weather domes or housings, checks on the functioning of the equipment, and any minor adjustments that need to be made to the equipment settings to maintain picture quality.

7.3.3. The maintenance will also include regular periodic overhaul of all the equipment and replacement of equipment, which is reaching the end of its serviceable life.

7.3.4. The maintenance agreement will also provide for 'emergency' attendance by a specialist CCTV engineer on site to rectify any loss or severe degradation of image or camera control.

7.3.5. The maintenance agreement will define the maximum periods of time permitted for attendance by the engineer and for rectification of the problem depending upon the severity of the event and the operational requirements of that element of the System.

7.3.6. It is the responsibility of the System Manager to ensure appropriate records are maintained in respect of the functioning of the cameras and the response of the maintenance organisation.

8. Access to and Security of the CCTV Control Room and Associated Equipment

8.1. Authorised Access

8.1.1. Only trained or authorised personnel will operate the equipment located within the CCTV control room, (or equipment associated with the System). This may include officers of the Metropolitan Police Service.

8.2. Public Access

8.2.1. Public access to the monitoring and recording facility will be prohibited except for lawful, proper and sufficient reasons and only then with the personal authority of the System manager. Any such visits will be conducted and recorded in accordance with the Procedural Manual.

8.3. Authorised Visits

8.3.1. Visits by inspectors do not fall into the scope of the above paragraph and may take place at any time, without prior warning. No more than TWO inspectors will visit at any one time. Inspectors will not influence the operation of any part of the System during their visit. The visit will be suspended in the event that it could disrupt the operational functioning of the control room. Any such visit should be recorded in the same way as that described above. Compliance auditing and visits by the Corporate Information Security Compliance Manager will occur as and when required, and without prior notice.

8.4. Declaration of Confidentiality

8.4.1. Regardless of their status, all visitors to the CCTV monitoring room, including inspectors and auditors, will be required to sign the visitors book, which includes a declaration of confidentiality.

8.5. Security

8.5.1. Authorised personnel will normally be present at all times when the equipment is in use. If the monitoring facility is to be left unattended for any reason it will be secured. In the event of the monitoring room having to be evacuated for safety or security reasons, the provisions of the Procedural Manual will be complied with.

8.5.2. The monitoring room will at all times be secured by 'Magnetic-Locks' operated by the CCTV Operator and 'digi-Locks' requiring a numeric code for entrance. The codes will be changed whenever there is a change in personnel.

9. Management of Recorded Material

9.1. Guiding Principles

9.1.1. For the purposes of this Code 'recorded material' means any material recorded by, or as the result of, technical equipment which forms part of the System, but specifically includes images recorded digitally.

9.1.2. Every digital recording obtained by using the System has the potential to be admitted in evidence at some point during its life span.

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

9.1.4. It is therefore of the utmost importance that irrespective of the means or format of the images obtained from the system, they are treated strictly in accordance with this Code and the Procedural Manual from the moment they are received by the monitoring room until final destruction or erasure. Every movement and usage will be meticulously recorded.

9.1.5. Access to and use of recorded material will be strictly for the purposes defined in this Code.

9.1.6. Recorded material will not be copied, sold, otherwise released or used for commercial purposes or for the provision of entertainment.

9.2. Release of Data to a Third Party

9.2.1. Every request for the release of personal data generated by the System will be referred to the Head of Governance, Systems Performance and Customer Experience Customer Services and ICT Strategy.

9.2.2. In complying with the Data Protection Act 2018 and GDPR 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:

- Recorded material shall be processed lawfully and fairly, and used only for the purposes defined in this Code.
- Access to recorded material will only take place in accordance with the standards outlined in this Code.
- The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

9.2.3. Members of the police service or other agency having a statutory authority to investigate and / or prosecute offences may, subject to compliance with this Code, release details of recorded information to the media only in an effort to identify alleged offenders or potential witnesses.

9.2.4. If material is to be shown to witnesses, including police officers, for the purpose of obtaining identification evidence, it must be shown in accordance with this Code and the Procedural Manual.

9.2.5. It may be beneficial to make use of recorded material for the training and education of those involved in the operation and management of CCTV systems, and for those involved in the

investigation, prevention and detection of crime. Any material recorded by virtue of the System will only be used for such bona fide training and education purposes. Recorded material will not be released for commercial or entertainment purposes.

9.3. Primary Requests to View Data

9.3.1. Primary requests to view data generated by the System are likely to be made by third parties for one or more of the following purposes:

I. Providing evidence in criminal proceedings.
II. The investigation, prevention and detection of crime (may include the identification of offenders).
III. Identification of witnesses.

9.3.2. Third parties, which are 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.

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

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, but which may be pending application for, or the issue of, a court order or subpoena. A time limit shall be imposed on such retention, which will be notified at the time of the request.

9.4. Secondary Requests to View Data

9.4.1. 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 shall ensure that:

I. The request does not contravene, and compliance with the request would not breach, current relevant legislation, (e.g. Data Protection Act 2018, GDPR, Human Rights Act 1998, 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 2018 and GDPR).
III. Due regard has been taken of any relevant case law.
IV. The request would pass a test of 'disclosure in the public interest'.

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

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 this Code.
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 a senior officer within the Local Authority. The officer should have personal knowledge of the potential benefit to be derived from releasing the material and an understanding of this Code.

9.5. Recorded Information – Provision and Quality

9.5.1. To ensure the quality of the recorded information, and that recorded information will meet the criteria outlined by current Home Office guidelines, the only disks to be used with the system are those, which have been specifically provided for this purpose.

9.6. Retention

9.6.1. Recorded information will be retained for no more than THIRTY-ONE DAYS, unless required for evidential purposes. The information will then be over written by the System.

9.7. Evidence Register

9.7.1. Evidential material will have a unique tracking record maintained in accordance with the procedural manual, which will be retained for at least three years.

9.8. Recording Policy

9.8.1. Subject to the equipment functioning correctly, images from each camera will be recorded throughout every 24-hour period onto digital recorders known as Primary Storage Nodes.

9.9. Evidential Material

9.9.1. In the event of recordings being required for evidential purposes the procedures outlined in the Procedural Manual will be strictly complied with.

10. Video Prints

10.1. Guiding Principles

10.1.1. A video print is a copy of an image or images which exists on computer disk. Such prints are within the definitions of 'data' and recorded material.

10.1.2. Video prints will not be taken as a matter of routine. 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 Procedural Manual.

10.1.3. Video prints contain data and will therefore only be released under the terms of this Code. If prints are released to the media in an effort to identify alleged offenders or potential witnesses, full details will be recorded in accordance with the Procedural Manual.

10.1.4. A record will be maintained of all video print productions in accordance with the Procedural Manual. The recorded details will include: a sequential 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) and the purpose for which the print was taken.

10.1.5. The records of the video prints taken will be subject to audit in common with all other records in the system.

Appendix A: Key Personnel and Responsibilities

1. System Owners

Representative:
Ray Seabrook – Assistant Director of Community Safety & Environment
Tel: 020 8921 3131

Responsibilities:
This role includes responsibility to:

I. Ensure the provision and maintenance of all equipment forming part of the System in accordance with contractual arrangements, which the owners may from time to time enter into.
II. Maintain close liaison with the System Manager.
III. Ensure the interests of the owners and other organisations are upheld in accordance with the terms of this Code.
IV. Agree to any proposed alterations and additions to the system, this Code and / or the Procedural Manual.

2. System Management

Representative:
Lorraine Hancock - CCTV System Assistant Manager
Tel: 020 8921 2028
Dave Downs – CCTV System Manager
Tel:020 8921- 4645

Responsibilities:
This role includes responsibility to:

I. Maintain day-to-day management of the System and staff.
II. Accept overall responsibility for the system and for ensuring that this Code is complied with.
III. Maintain direct liaison with the owner of the System.
IV. Maintain direct liaison with operating partners.

3. Data Protection

Representative:
Corporate Data Guardian - Customer Services and ICT Strategy
Tel: 020 8921 2383

Responsibilities:
This role includes responsibility to:

I. Ensure compliance with the Data Protection Act 2018 and GDPR.
II. Manage the Subject Access process.
III. Perform compliance auditing of the System.

Appendix B: Extracts from Data Protection Act 2018 and GDPR

Section 7

(1) Subject to the following provisions of this section and to sections 8 and 9, an individual is entitled:
- (a) to be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller.
- (b) if that is the case, to be given by the data controller a description of:
  - (1) the personal data of which that individual is the data subject;
  - (2) the purpose for which they are being or are to be processed;
  - (3) the recipients or classes of recipients to whom they are or may be disclosed,
- (c) to have communicated to him in an intelligible form:
  - (1) the information constituting any personal data of which that individual is the data subject;
  - (2) any information available to the data controller as the source of those data; and
- (d) where the processing by automatic means of personal data of which that individual is the data subject for the purposes of evaluating matters relating to him such as, for example, his performance at work, his creditworthiness, his reliability or his conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him, to be informed by the data controller of the logic involved in that decision-taking.

(2) A data controller is not obliged to supply any information under subsection
- (a) Unless he has received:
  - (1) A request in writing, and
  - (2) Except in prescribed cases, such fee (not exceeding the prescribed maximum) as he may require.

(3) A data controller is not obliged to comply with a request under this section unless he is supplied with such information as he may reasonably require in order to satisfy him as to the identity of the person making the request and to locate the information which that person seeks.

(4) Where a data controller cannot comply with the request without disclosing information relating to another individual who can be identified from that information, he is not obliged to comply with the request unless:
- (a) the other individual has consented to the disclosure of the information to the person making the request, or
- (b) it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

(5) In subsection (4) the reference to information relating to another individual includes a reference to information identifying that individual as the source of the information sought by the request; and that subsection is not to be construed as excusing a data controller from communicating so much of the information sought by the request as can be communicated without disclosing the identity of the other individual concerned, whether by the omission of names or other identifying particulars or otherwise.

(6) In determining for the purposes of subsection (4)(b) whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned, regard shall be had, in particular, to:
    (a) any duty of confidentiality owed to the other individual,
    (b) any steps taken by the data controller with a view to seeking the consent of the other individual,
    (c) whether the other individual is capable of giving consent, and
    (d) any express refusal of consent by the other individual.

(7) An individual making a request under this section may, in such cases as may be prescribed, specify that his request is limited to personal data of any prescribed description.

(8) Subject to subsection (4), a data controller shall comply with a request under this section promptly and in any event before the end of the prescribed period beginning with the relevant day.

(9) If a court is satisfied on the application of any person who has made a request under the foregoing provisions of this section that the data controller in question has failed to comply with the request in contravention of those provisions, the court may order him to comply with the request.

(10) In this section:
    (a) 'prescribed' means prescribed by the Secretary of State by regulations;
    (b) 'the prescribed maximum' means such amount as may be prescribed;
    (c) the prescribed period' means forty days or such other period as may be prescribed;
    (d) 'the relevant day', in relation to a request under this section, means the day on which the data controller receives the request or, if later, the first day on which the data controller has both the required fee and the information referred to in subsection (3).

(11) Different amounts or periods may be prescribed under this section in relation to different cases.

Section 8

(1) The Secretary of State may by regulations provide that, in such cases as may be prescribed, a request for information under any provision of subsection (1) of section 7 is to be treated as extending also to information under other provisions of that subsection.

(2) The obligation imposed by section 7(1)(c)(i) must be complied with by supplying the data subject with a copy of the information in permanent form unless:
    (a) the supply of such a copy is not possible or would involve disproportionate effort, or
    (b) the data subject agrees otherwise;
    and where any of the information referred to in section 7(1)(c)(i) is expressed in terms which are not intelligible without explanation the copy must be accompanied by an explanation of those terms.

(3) Where a data controller has previously complied with a request made under section 7 by an individual, the data controller is not obliged to comply with a subsequent identical or similar request under that section by that individual unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request.

(4) In determining for the purposes of subsection (3) whether requests under section 7 are made at reasonable intervals, regard shall be had to the nature of the data, the purpose for which the data are processed and the frequency with which the data are altered.

(5) Section 7(1)(d) is not to be regarded as requiring the provision of information as to the logic involved in decision-taking if, and to the extent that, the information constitutes a trade secret.

(6) The information to be supplied pursuant to a request under section 7 must be supplied by reference to the data in question at the time when the request is received, except that it may take account of any amendment or deletion made between that time and the time when the information is supplied, being an amendment or deletion that would have been made regardless of the receipt of the request.

(7) For the purposes of section 7(4) and (5) another individual can be identified from the information being disclosed if he can be identified from that information, or from that and any other information which, in the reasonable belief of the data controller, is likely to be in, or to come into, the possession of the data subject making the request.

Appendix C: Restricted Access Notice

WARNING

RESTRICTED ACCESS AREA

Everyone, regardless of status, entering this area is required to complete an entry in the Visitors book.

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 acknowledge that the precise location of the CCTV monitoring 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 Visitors book is your acceptance of these terms'.

Appendix D: Declaration of Confidentiality

Royal Borough of Greenwich CCTV System

I, ..., am retained by the Royal Borough of Greenwich to perform the duty of CCTV Control Room Operator. I have received a copy of the Code of Practice in respect of the operation and management of that Community Safety CCTV System.

I hereby declare that:

I am fully aware of the content of the Code of Practice and understand that all duties which I undertake in connection with the Community Safety CCTV System must not contravene any part of the current Code of Practice, or any future amendments of which I am made aware. If now, or in the future, I am or become unclear of any aspect of the operation of the System or the content of The Code of Practice, I undertake to seek clarification of any such uncertainties.

I understand that it is a condition of my employment that I do not disclose or divulge to any individual, firm, company, authority, agency or other organisation, any information which I may have acquired in the course of, or for the purposes of, my position in connection with the Community Safety CCTV System, verbally, in writing or by any other media, now or in the future, (including such time as I may no longer be retained in connection with the Community Safety CCTV System). In appending my signature to this declaration, I agree to abide by the Code of Practice at all times.

I further acknowledge that I have been informed and clearly understand that the communication, either verbally or in writing, to any unauthorised person(s) of any information acquired as a result of my employment with the Royal Borough of Greenwich may be treated as non-compliance with the Code of Practice and may be considered a breach of discipline and dealt with accordingly, including, if appropriate, the instigation of criminal proceedings.

Signed: ..... Print: .....

Witness: ..... Position: .....

Dated this ..... day of ..... (month) ..... (year)

Appendix E: Inspector's Declaration of Confidentiality

In Respect of Royal Borough of Greenwich CCTV System

I, ..., am a voluntary inspector of the Royal Community Safety CCTV System with a responsibility to monitor the operation of the Community Safety CCTV System and adherence to the Code of Practice. I have received a copy of the Code of Practice in respect of the operation and management of that Community Safety CCTV System.

I hereby declare that:

I am fully conversant with my voluntary duties and the content of that Code of Practice. I undertake to inform the System Manager of any apparent contraventions of the Code of Practice that I may note during the course of my visits to the monitoring facility.

If now, or in the future I am, or I become unclear of any aspect of the operation of the System or the content of The Code of Practice, I undertake to seek clarification of any such uncertainties.

I understand that it is a condition of my voluntary duties that I do not disclose or divulge to any firm, company, authority, agency, other organisation or any individual, any information which I may have acquired in the course of, or for the purposes of, my position in connection with the Community Safety CCTV System, verbally, in writing or by any other media, now or in the future, (including such time as I may no longer be performing the role of inspector). In appending my signature to this declaration, I agree to abide by the Code of Practice at all times.

Signed: ..... Print: .....

Witness: ..... Position: .....

Dated this ..... day of ..... (month) ..... (year)

Appendix F: Subject Access Request Form - Example

DATA SUBJECT ACCESS CCTV APPLICATION FORM

ROYAL borough of GREENWICH

Under the terms of the Data Protection Act 2018 and GDPR, an individual is entitled to ask the authority for a copy of
all the personal information which it holds about him/her for the purposes of providing services to the individual. The information, which the individual is entitled to receive from the authority, includes a description of these purposes and the recipients to whom the data can be disclosed. This entitlement is known as the "Right of Access to Personal Data". Please complete this form, providing as much information as possible, should you wish to exercise your right in requesting disclosure of your data.

PLEASE NOTE THAT RECORDED DATA IS ONLY HELD FOR 31 DAYS BEFORE IT IS DELETED

1. PERSONAL DETAILS

Name:			
Address:			
Telephone Number:		E-mail Address:	
Gender:			

2. INFORMATION REQUIRED

To help us find the CCTV data you require, please complete the following section.			
Date:		Time:	
Location:			
Description of Incident			