



Southampton City Council

Closed Circuit Television (CCTV) Code of Practice

Version 3

April 2013

THE CODE OF PRACTICE FOR THE OPERATION OF CCTV IN SOUTHAMPTON

CONTENTS

Section 1 Introduction and Objectives

- 1.1 Introduction
- 1.2 Statement in respect of the Human Rights Act 1998
- 1.3 Objectives of the System
- 1.4 Operational Procedures

Section 2 Statements of Purpose and Principle

- 2.1 Purpose
- 2.2 General principles of Operation
- 2.3 Copyright
- 2.4 Cameras and coverage
- 2.5 Monitoring and recording facilities
- 2.6 Human resources
- 2.7 Processing and handling of recorded material
- 2.8 Operators' instructions
- 2.9 Changes to the Code or Operating Procedure

Section 3 Privacy and data protection

- 3.1 Public concern
- 3.2 Data Protection Act 1998
- 3.3 Requests for information
- 3.4 Exemptions to the provision of information

Section 4 Accountability and public information

- 4.1 The public

Section 5 Control and Operation of cameras

- 5.1 Guiding principles
- 5.2 Primary control
- 5.3 Operational command of the System by the police
- 5.4 Maintenance of the System

Section 6 Access to and security of the Control Room and associated equipment

- 6.1 Public access
- 6.2 Visitors' Book
- 6.3 Security

Section 7 Management of recorded material

- 7.1 Guiding principles
- 7.2 National standard for the release of data to third parties
- 7.3 Evidential images
- 7.4 Hard disk drive, CD ROM and DVD – provision and quality

Section 8 Prints

- 8.1 Guiding principles

Schedule 1 Key personnel and responsibilities

Schedule 2 Operational procedures

Schedule 3 Complaints procedures

Appendix A Release of data to third parties

Appendix B Declaration of Confidentiality

Appendix C Subject Access Form

SECTION 1: INTRODUCTION AND OBJECTIVES

1.1 Introduction

- 1.1.1 Public realm CCTV in Southampton is operated by Balfour Beatty Living Places on behalf of Southampton City Council. Southampton City Council, Balfour Beatty Living Places and Hampshire Constabulary are committed to the improvement of community safety, crime prevention and maintaining the attractiveness of the city, as a place to live, visit for shopping, business and leisure. Southampton City Council, Balfour Beatty Living Places and Hampshire Constabulary have signed up to this Code of Practice and are confident that it will serve the community well.
- 1.1.2 This Code of Practice will apply equally to other CCTV systems operated by Southampton City Council departments.
- 1.1.3 The aim of this Code of Practice is to help employees operating Closed Circuit Television (CCTV) schemes monitoring members of the public to do so in full compliance of the Data Protection Act 1998, Human Rights Act 1998, Regulation of Investigatory Powers Act 2000 (RIPA) and in adherence to high standards of good practice as laid out by the Information Commissioner's Office. Compliance with this policy will not only help CCTV scheme operator's process personal data in compliance with the law but also help to maintain public confidence without which they cannot operate.
- 1.1.4 CCTV systems have been installed at the locations across the city. These systems, collectively known as 'the System', comprise a number of cameras installed at strategic locations. All the cameras are fully operational and are either fixed or pan, tilt and zoom.
- 1.1.5 For the purposes of this document, the 'owner' of the System is Southampton City Council ('the Council').
- 1.1.6 For the purposes of the Data Protection Act 1998, the Data Controller is Southampton City Council (who either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are to be processed.
- 1.1.7 The System Manager is Southampton City Council, except where contracted to a third party.
- 1.1.8 The System has been notified to the Information Commissioner's Office.
- 1.1.9 Details of key personnel, their responsibilities and contact points are shown in Schedule 1 of this Code of Practice (the 'Code').

1.2 Statement in respect of the Human Rights Act 1998

- 1.2.1 All parties recognise 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 Southampton is a necessary, proportionate and suitable tool to help reduce crime, reduce the fear of crime and improve community safety.
- 1.2.2 Section 163 of the Criminal Justice and Public Order Act 1994 creates the power for local authorities to provide CCTV coverage of any land within their area for the purposes of crime prevention or victim welfare and it is also considered a necessary initiative by Southampton City Council towards their duties under the Crime and Disorder Act 1998.
- 1.2.3 It is recognised that the operation of the System may be considered to infringe on the privacy of individuals. The parties recognise that it is its 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 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, for the protection of health and morals, or for the protection of the rights and freedoms of others.

- 1.2.4 The Code and observance of the Operational Procedures (Schedule 2) shall ensure that evidence is secured, retained and made available as required to ensure that there is absolute respect for everyone's right to a fair trial.
- 1.2.5 The System shall be operated with respect for all individuals, recognising the right to be free from inhumane or degrading treatment and avoiding discrimination as required, ensuring that there is absolute respect for everyone's right to a fair trial.
- 1.2.6 The System shall be operated with respect for all individuals, recognising the right to be free from inhumane or degrading treatment and avoiding discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

1.3 Objectives of the System

- 1.3.1 The objectives of the System as determined by Southampton City Council as the Data Controller, and which form the lawful basis for the processing of data are:
- To help reduce the fear of crime to provide a safe and secure environment for residents of, and visitors to, the areas covered by the scheme.
 - To help deter and detect crime and provide evidential material for court proceedings.
 - To assist in the overall management of Southampton City Council.
 - To assist in the management of Southampton City Council's Housing Stock covered by the Concierge Service.
 - To assist in the management of other locations and buildings owned or controlled by Southampton City Council.
 - To enhance community safety, including the prevention and detection of harassment, to assist in developing the economic well being of the Southampton area and encourage greater use of the city centre.
 - To assist the local authority in their enforcement and regulatory functions within the Southampton area.
 - To assist in traffic management, and encourage safer and more sustainable use of all modes of transport and provide travel information to the media and public.
 - To assist in supporting civil proceedings.
 - To identify breaches of tenancy terms and to supply evidence to support enforcement action, this may include civil proceedings.
 - To monitor all modes of travel to enable improvement and better management of the public highway (traffic cameras).
 - The scheme will operate in a manner that is sensitive to the privacy of people living and working in the area, and operate at all times within the Data Protection Act 1998, the Human Rights Act 1998 and Regulation of Investigatory Powers Act 2000.

1.4 Operational Procedures

- 1.4.1 The Code is supplemented by the Operational Procedures (Schedule 2) that offers instructions on all aspects of the day-to-day operation of the System. To ensure that the purpose and principles (Section 2) of the System are realised, the Operational Procedures are based and expanded upon the contents of the Code.
- 1.4.2 Under no circumstances will any operating camera be deliberately rendered inoperable, as to do so may compromise public safety and evidence gathering. There is no justification or legitimacy in law to be so directed. Any interference of this nature from whatever source should immediately be referred to the CCTV Manager.

SECTION 2: STATEMENTS OF PURPOSE AND PRINCIPLES

2.1 Purpose

- 2.1.1 The purpose of this document is to state the intention of the owners and the managers as listed in Schedule 1, on behalf of the parties involved, and as far as is reasonably practicable, to support the objectives of the System, and to outline how it is intended to do so.
- 2.1.2 The purpose of the System and the process in determining the reasons for implementing the System is as previously defined in order to achieve the key 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 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 1998 at all times.
- 2.2.4 The System will be operated in accordance with the Public Order Act 1986 with particular regard to section 5 – Harassment (where applicable).
- 2.2.5 The System will be operated fairly, within the law, and only for the objectives for which it was established. These purposes are identified as 1.3 of the Code.
- 2.2.6 The System will be operated with due regard to the principle that everyone has the right to respect for his or her private and family life and their home.
- 2.2.7 The public interest in the operation of the System will be recognised by ensuring the security and integrity of Operational Procedures. Throughout the Code it is intended, as far as is reasonably possible, to balance the objectives of the System with the need to safeguard the individual's rights. Every effort has been made throughout the Code to indicate that a formal structure has been put in place, including a complaints procedure, Schedule 3, by which it can be identified that the System is not 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 the Code and to be accountable under it.

2.3 Copyright

- 2.3.1 Copyright 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 the System to which the Code refers are the public areas within the responsibility of the operating partners and cover the Southampton boundary.
- 2.4.2 None of the cameras forming part of the System are installed in a covert manner.
- 2.4.3 Signs have been erected to indicate to members of the public that they are entering a zone covered by Closed Circuit Television (CCTV). Signs that CCTV cameras are operating will be displayed at key positions where the scheme is operating. All enquiries should be made in accordance with the contact telephone number on the sign.
- 2.4.4 Most pictures captured on camera will be transmitted to a central control room where they will be recorded in accordance with the Code.
- 2.4.5 To ensure privacy, the cameras will only monitor those spaces, which are defined under the Council's Notification of the system to the Information Commissioner's Office. Equipment will be operated with high regard for the privacy of the individual.

- 2.4.6 Cameras will not look into private property. The Council is under an obligation to ensure that the Operational Procedures (Schedule 2) and technological measures that are adopted impose restraints upon the use of cameras in connection with private premises.
- 2.4.7 Most of the System is in operation 24 hours per day, 365 days of the year, with pictures being continuously monitored and recorded.
- 2.4.8 In addition, the Council's Control Room at City Depot provides a feed to the Hampshire Constabulary Control Room to allow the police to view incidents, captured by the Control Room. There is also a feed to St Mary's Stadium which is governed by the *Data Sharing Agreement between Southampton City Council and Southampton Football Club Ltd*. West Quay Retail Park also provides feeds into the Control Room.
- 2.4.9 Although every effort has been made in the planning and design of the CCTV systems to give them maximum effectiveness, it is not possible to guarantee that the System will detect every incident taking place within the area of coverage.

2.5 Monitoring and recording facilities

- 2.5.1 The CCTV equipment used by the two main Control Rooms records footage simultaneously throughout every 24 hour period.
- 2.5.2 CCTV Operators are able to record images from selected cameras in real-time, produce hard copies of recorded images, replay, or copy any pre-recorded data at their discretion and in accordance with the Code. All viewing and recording equipment shall only be operated by trained and authorised users.
- 2.5.3 Dedicated picture and telephone links between City Depot Control Room and the police control room have been provided. These will be used to relay information on incidents that arise and to communicate information. Camera control and picture recording facilities have not been provided for police use.

2.6 Human resources

- 2.6.1 Unauthorised persons will not have access to the Control Room without an authorised member of staff being present.
- 2.6.2 Only specially selected and trained Operators in accordance with the Operational Procedures shall staff the Control Room.
- 2.6.3 All staff are aware of the sensitive nature of the pictures with which they are dealing and are fully conversant with the procedures required for access to recorded images by Data Subjects.
- 2.6.4 The CCTV Manager will ensure that new and relief staff are fully briefed and trained on all functions, operational and administrative, arising within the CCTV Control Room operation.
- 2.6.5 In the interest of efficient co-operation, Control Room staff are familiar with the police operation and reciprocal arrangements have been made for the police staff to visit the CCTV Control Room to familiarise themselves with working procedures.
- 2.6.6 All staff must have appropriate checks, prior to commencing work.

2.7 Processing and handling of recorded material

- 2.7.1 All recorded material, in whatever form, will be processed and handled by all Parties strictly in accordance with the Code and the Operational Procedures (Schedule 2).

2.8 Operators' instructions

- 2.8.1 Technical instructions on the use of equipment housed within the Control Room are contained in separate manuals provided by the equipment suppliers within the Control Room.

2.9 Changes to the Code or Operational Procedures

- 2.9.1 Any major changes to either the Code or the Operational Procedures (i.e. such as will have a significant impact upon the Code or upon the operation of the System) will take place only upon agreement being reached between the parties.

SECTION 3: PRIVACY AND DATA PROTECTION

3.1 Public concern

- 3.1.1 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.
- 3.1.2 The data will be securely stored strictly in accordance with the requirements of the Data Protection Act 1998 and any additional locally agreed procedures.

3.2 Data Protection Act 1998

- 3.2.1 The operation of the System has been notified to the Information Commissioner's Office in accordance with current Data Protection legislation.
- 3.2.2 The Data Controller for the System is Southampton City Council.
- 3.2.3 All data will be processed in accordance with the principles of the Data Protection Act 1998. The principles include:
- i) All personal data will be obtained and processed fairly and lawfully
 - ii) Personal data will be held only for the purposes specified
 - iii) Personal data shall be adequate, relevant and not excessive
 - iv) Personal data shall be accurate and where necessary, kept up to date
 - v) Personal data shall not be kept for longer than is necessary
 - vi) Personal data shall be processed in accordance with the rights of the data subjects
 - vii) Appropriate security measures must be in place to ensure against accidental loss or destruction of, or damage to, personal data
 - viii) Personal data shall not be transferred to a country outside of the European Economic Area unless that country has adequate levels of protection for the rights and freedoms of Data Subjects.

3.3 Requests for information

- 3.3.1 Any request from an individual for the access to personal data that he/she believes is recorded by virtue of the System will be directed in the first instance to the council's Information Compliance officer.
- 3.3.2 If the request cannot be complied with without identifying another individual, where appropriate, permission from all such other 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.
- 3.3.3 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 C.

3.4 Exemptions to the provision of information

- 3.4.1 In considering a request made under the provision of Section 7 of the Data Protection Act 1998, reference may also be made to Section 29 of the Act which includes the following statement: Personal data processed for the following purposes namely:
- i) the prevention or detection of crime
 - ii) the apprehension or prosecution of offenders
- is exempt from the Subject Access provision 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'.

SECTION 4: ACCOUNTABILITY AND PUBLIC INFORMATION

4.1 The public

- 4.1.1 For reasons of security and confidentiality, access to the Control Room is restricted.
- 4.1.2 Cameras will not be used to look into private residential property. The Operators will be specifically trained in privacy issues.
- 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 appropriate CCTV Manager. All complaints shall be dealt with in accordance with Southampton City Council's Corporate Complaints procedure (Schedule 3).
- 4.1.4 All CCTV staff are contractually subject to regulations governing confidentiality and discipline.

SECTION 5: CONTROL AND OPERATION OF CAMERAS

5.1 Guiding principles

- 5.1.1 Any person operating the cameras will act with utmost integrity at all times.
- 5.1.2 The cameras, control equipment, recording and reviewing equipment shall at all times only be operated by persons who have been trained in their use and the legislative implications of their use.
- 5.1.3 Every use of the cameras will accord with the purposes and key objectives (See section 1.3 and 2.1 above) of the System and shall be in compliance with the Code.
- 5.1.4 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 CCTV Manager.

5.2 Primary control

- 5.2.1 Only those trained and authorised members of staff with responsibility for using CCTV equipment will have access to the operating controls – those Operators have primacy of controls at all times.

5.3 Operational command of the System by the police

- 5.3.1 Under rare and extreme operational circumstances, the police may make a request to command the use of the System to which this Code applies. These circumstances may be a major incident or event that has a significant impact on the prevention and detection of crime or public safety. Such use will provide the police with a broad overview of events in order to command the incident.
- 5.3.2 Such requests will be viewed separately to the use of the System's cameras with regard to the requirement for an authority for specific types of surveillance under the Regulation of Investigatory Powers Act 2000. (Please refer to *Southampton City Council Corporate Surveillance Guidance*).
- 5.3.3 Applications made as at 5.3.1 and 5.3.2 above will be considered on the written request of a police officer not below the rank of Superintendent. In the event of an urgent need, a verbal request of the senior officer in charge, and in any case an officer not below the rank of Inspector, will be necessary. This should be followed as soon as practicable within 72 hours by a superintendent's written request.
- 5.3.4 In the event of such a request being permitted, the Control Room will continue to be staffed, and equipment operated by only those personnel who are specifically trained to do so, and who fall within the terms of Sections 6 and 7 of the Code. They will then operate under the command of the police officer designated in the verbal/written request, taking into account their responsibilities under this Code.
- 5.3.5 In very extreme circumstances, a request may be made for the police to take control of the System in its entirety, including the staffing of the Control Room and personal control of all associated equipment, to the exclusion of all representatives of the System owners. Any such request should be made to the appropriate CCTV 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.

5.4 Maintenance of the System

- 5.4.1 To ensure compliance with the Information Commissioner's Code of Practice which states that images recorded must continue to be of appropriate evidential quality, the System shall be maintained under a local maintenance agreement.
- 5.4.2 The maintenance agreement should make provision for regular/periodic service checks on the equipment which will include cleaning of any all-weather domes or housings check on the functioning of the equipment, and any minor adjustments that need to be made to the equipment settings to maintain picture quality.
- 5.4.3 The maintenance will also include regular periodic overhaul of all the equipment and replacement of equipment that is reaching the end of its serviceable life.
- 5.4.4 Upon installation, all equipment is checked to ensure that it is performing within specification.
- 5.4.5 The System comprises of fixed, pan, tilt and zoom cameras, multiplex and real time monitors, time lapse and real time recording and playing equipment and any other ancillary equipment including equipment connected with the transmission of pictures from mobile CCTV locations.
- 5.4.6 A schedule is in place to check that all cameras are operating correctly, and if a fault is detected then it is recorded in the maintenance log for repair. This log records the time and date of the repair.
- 5.4.7 Most cameras are housed in vandal proof housings with either clear or smoked domes for protection.

SECTION 6: ACCESS TO AND SECURITY OF THE CONTROL ROOM AND ASSOCIATED EQUIPMENT

6.1 Public access

- 6.1.1 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 CCTV Manager. Any such visits will be conducted and recorded in accordance with the Operational Procedures.

6.2 Visitors' Book

- 6.2.1 A Visitors' Book will be maintained, and visitors will be required to complete the book in the interests of propriety and Health and Safety regulations.

6.3 Security

- 6.3.1 Authorised personnel will normally be present at all times when the equipment is in use. If the Control Room facility has to be left unattended for any reason, it will be secured.
- 6.3.2 The Control Room will at all times be secured by appropriate secure means.

SECTION 7: MANAGEMENT OF RECORDED MATERIAL

7.1 Guiding principles

- 7.1.1 For the purpose of the 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.
- 7.1.2 Every digital recording obtained by using the System has the potential of containing material that has to be admitted in evidence at some point during its lifespan.
- 7.1.3 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 the Code and the Operating Procedures from the moment they are received by the Control Room until final destruction. Every movement and usage will be recorded.
- 7.1.4 Access to and the use of recorded material will be strictly for the purposes defined in the Code only.
- 7.1.5 Recorded material will not be copied, sold, otherwise released or used for commercial purposes or for the provision of entertainment.

7.2 National standard for the release of data to a third party

- 7.2.1 Every request for the release of personal data generated by the System will be channelled through the CCTV Manager or on duty supervisor.
- 7.2.2 In complying with this Code 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 the Code;
Access to recorded material will only take place in accordance with the standards outline in Appendix A and the Code;
The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.
- 7.2.3 Members of the police force or other agencies who have a statutory authority to investigate and/or prosecute offenders 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.
- 7.2.4 It may be beneficial to make use of 'real' digital footage for the training and education of Southampton City Council staff in the operation and management of the System. Any material recorded by virtue of the System will only be used for such bona fide training and education purposes of Southampton City Council staff, and will only be used in accordance with the law.

7.3 Evidential images

- 7.3.1 In the event of recording being required for evidential purposes, the procedures outlined in the Operational Procedures will be strictly complied with.

7.4 Hard disk drive, CD ROM and DVD – provision and quality

- 7.4.1 To ensure the quality of the hard disk drive, CDs and DVDs and that the recorded information will meet the criteria outline by the current Home Office guidelines, the only recording medium to be used with the System are those which have been specifically provided in accordance with the Operational Procedures.

SECTION 8: PRINTS

8.1 Guiding principles

- 8.1.1 A print is a copy of an image or images that already exist on the System. Such prints are equally within the definitions of 'data' and recorded material.
- 8.1.2 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 Operational Procedures.
- 8.1.3 Prints contain data and therefore can only be released under the terms of Appendix A to the Code, 'Release of data to third parties'. If prints are released to the media (in compliance with Appendix A) in an effort to identify alleged offenders or potential witnesses, full details of the disclosure will be recorded in accordance with the Operational Procedures.
- 8.1.4 A record will be maintained of all print productions in accordance with the Operational Procedures.
- 8.1.5 The records of the prints taken will be subject to audit in common with all other records in the System.

SCHEDULE 1: KEY PERSONNEL AND RESPONSIBILITIES

1. Information Compliance officer
Corporate Legal Team
Southampton City Council
Civic Centre
Southampton
SO14 7LY
Tel: 023 8083 2676
Email: foi.requests@southampton.gov.uk

2. Citywatch
CCTV Control Room
Balfour Beatty Living Places
City Depot
First Avenue
Millbrook
Southampton
SO15 0LJ
Tel: 023 8079 8100
Email: citywatch@bblivingplaces.com

3. Concierge Service
Operations Manager
Housing Services
Southampton City Council
City Depot
First Avenue
Millbrook
Southampton
SO15 0LJ
Tel: 023 8083 4566
Email: concierge@southampton.gov.uk

4. Civic Buildings
Civic Buildings Manager
Southampton City Council
Civic Centre
Southampton
SO14 7LY
Tel: 023 8083 2877
Email: civic.buildings@southampton.gov.uk

Responsibilities

The CCTV Manager is responsible for the day-to-day operational management of the System.

The role of the CCTV Manager includes responsibility to:

- i. Maintain day-to-day management of the System and the staffing contract.
- ii. Ensure that the Code is complied with on a day-to-day basis.
- iii. Maintain direct liaison with relevant operating partners.

SCHEDULE 2: OPERATIONAL PROCEDURES

Introduction

These Operational Procedures have been drawn up in conjunction with the CCTV Code of Practice 'the Code' which sets out minimum standards expected of all employees and authorised users managing and operating the System. The efficient and legal operation of CCTV rests with the standards contained within the Code. It should be considered as a benchmark for good practice that will ensure accountability and command employee and public confidence.

The Code will be the principal document for the resolution of any difficulties or discrepancies that may arise from the operation of the System.

The Code together with these Operational Procedures will be subject to amendments and updates as required. It is the responsibility of all staff working with the System to ensure that at all times they adhere to the contents of these documents. The documents have been written against the legal requirements of the Human Rights Act 1998. It is incumbent upon all staff to draw to the attention of the Data Controller any departure from the terms of the Code or its related Operational Procedures.

a. Operator duties and responsibilities

The very nature of CCTV is that it poses an intrusive breach of an individual's privacy. The majority of those who visit or pass by cameras will do so without an understanding of the range and capability of the cameras. The parties recognise the very real position and trust that those who operate the System have. In recognising the legal requirements of the Human Rights Act 1998, the Data Protection Act 1998 and the Regulation of Investigatory Powers Act 2000, the parties have sought to provide those who operate the System with clear guidance on their duties and responsibilities.

b. Purposes of the System

The System must not be used for any purpose other than those defined in the Code (see 1.3 and 2.1 of the Code). Any failure to follow the Code will result in disciplinary action being taken against members of staff. In the context of the defined purposes of the System the cameras can be used in the detection of criminal activity as well as for the safety of people visiting and working in the area immediately covered by the camera.

c. System integrity

The CCTV Operators should have regard for the safety and well being of those using the areas covered by the cameras. In particular the individual's right to privacy must not be unduly infringed. To this end all Operators are required to:

Sign a Declaration of Confidentiality that will remain in force throughout their period of employment;

Undergo a period of training on the operation of the System and its related procedures;

Know the contents of the Code and these Operating Procedures;

Be aware at all times of the potential abuse there may be in operating the System;

e.g. looking into private areas such as office windows or people in their vehicles, unless such actions are justified through prior information;

Attend court as required to support evidence that might have been gathered in the course of their duties.

d. Selection and recruitment

The CCTV monitoring equipment is located within the Control Room and Operators are selected and recruited specifically for the role of monitoring the System.

Each Operator will be subject to a security vet and will be expected to demonstrate their understanding and commitment to total confidentiality at all times.

e. Training

The training required by a CCTV Operator will include company related information as well as technical and legal information. Operators will be provided with training in using the System. They will be encouraged to undertake further training to industry recognised standards. As such the Operators must know: The technical operation of the System including any training given by the equipment manufacturers and installers;

How to interpret the Code and related Operational Procedures;

The geographical location and coverage of every camera in the System;

The legal issues surrounding privacy and potential contravention of the Human Rights Act 1998, the Data Protection Act 1998 and the Regulation of Investigatory Powers Act 2000.

f. Discipline

CCTV Operators will be subject to relevant discipline codes. Any breach of these Operational Procedures, the Code or confidentiality will be dealt with in accordance with those discipline regulations and staff must recognise that any such breach may amount to gross misconduct, which could lead to dismissal.

All parties will accept prime responsibility for ensuring that there is no breach of security and that the Code and Operational Procedures are complied with. Those having day-to-day responsibility for the management of the Control Room will also have responsibility for enforcing the discipline regulations.

g. Duties of an Operator

Duties and responsibilities within the Control Room will be co-ordinated by the CCTV Manager and may vary on a daily basis in order of priority as incidents occur.

h. General duties

Keep a keen observation on the System's cameras.

Maintain an accurate and up to date log of events and occurrences

Only allow authorised personnel into the Control Room.

Use initiative and resourcefulness to deal with any situations that may arise and utilise available staff to the best possible use.

Carry out emergency procedures as directed in the relevant Emergency Procedures or by Hampshire Constabulary.

i. Responsibilities

Staff the Control Room at all times.

Maintain a constant watch over the areas covered by the System.

React promptly and correctly to warnings and indications given by any alarm systems installed ensuring that the action taken is logged.

Record details of all significant occurrences in the relevant log.

Answer all telephone calls in the correct manner and act upon them appropriately and efficiently.

Control the entry of people to the Control Room and only allow authorised personnel entry into these areas.

Maintain cleanliness and tidiness in the Control Room at all times.

Use initiative and resourcefulness to deal with situations that may arise and utilise available staff to the best use possible.

Ensure that all logs are kept up-to-date and information required is entered.

Take charge of keys and issue them only to the authorised personnel as directed by the CCTV Manager.

Ensure that correct and precise information is given to colleagues on handover.

Operating Procedures

a. Guiding principles

The Operators of the cameras and associated equipment will act with the utmost probity in the execution of their duty.

Every use of the cameras shall accord with the purposes and key objectives of the scheme and shall comply with the Code and the Operational Procedures.

Cameras will not be used to look into "private areas". Operators have been specifically trained in privacy issues.

Operators should be aware of exercising prejudices that may lead to complaints of the System being used for which it is intended. The Operators may have to justify their interest in, or recording of, any particular individual, group of individuals or property at any time by virtue of the System.

b. Observations

Operators should be alert but not exclusively, to the following activity:

Individuals acting suspiciously.

Groups of people and unaccompanied or vulnerable children (especially under 8 years old).

A person being escorted against their will.

Suspicious packages.

A Vehicle parked/broken down in a dangerous place.

Police and other emergency vehicles (particularly at access points).

c. Specific actions

If an incident occurs that is of a criminal nature, inform the police via the appropriate communications channel.

If emergency services (fire, ambulance or other similar organisations) are required to attend the premises then call them via the appropriate communications channel.

For all of the above, ensure that any recordings made are in "real time" and that the situation is closely monitored to ensure that the appropriate standard of images is recorded.

If a criminal activity is suspected of being monitored, the Operator should try to zoom the camera to obtain an 'identification' standard recording. Identification is where at least half of the subjects' body fills the screen.

After a good clear view has been obtained, the Operator should zoom the camera out to get a wider shot of the action. Wherever possible the subject(s) of the recording should be kept in the centre of the picture.

Other cameras should be manoeuvred to obtain a recording from a different angle.

All incidents should be recorded even if the police or other resources do not attend. The Operator will indicate the resources attending and in what numbers.

A record of the Occurrence form is to be completed in detail.

d. Access to the Control Room

Access to the Control Room is strictly controlled and only authorised persons are entitled to be in the Control Room. A list of those authorised to enter the Control Room is available at the site.

Under no circumstances should anyone else be in the Control Room without an authorisation from the CCTV Manager or designated deputy.

Physical proof of ID and the visitor's authorisation will be checked. Only when this is done will anyone be allowed entry into the Control Room.

Upon entry to the Control Room it is the Operators responsibility to ensure that all visitors sign in and when leaving sign out, recording each visitor's name, time of entry and exit and purpose of visit.

The Control Rooms are situated within secure premises and have separate security systems for entry to the premises. Controls and procedures will ensure no unauthorised access.

A Visitors' Book will be maintained, and visitors will be required to complete the book in the interests of propriety and Health and Safety Regulations.

A log will be maintained throughout operations. Brief details of incidents will be noted together with the action taken and results and stored on the System.

e. System check

System check forms are kept at the Control Room.

At the takeover of duty, the Operator will carry out a functional test of all the cameras, checking that all of the operating functions are working correctly. The results of this test must be recorded on the System Check form provided.

The Operator must fill in the form and describe any faults in detail.

The Control Room Supervisor will inspect all forms on a daily basis and ensure that action is being taken to rectify the problem.

Only copies of the System Check form can be removed from the Control Room. The original must remain in the Control Room.

f. Recording equipment

The System will record images digitally 24 hours per day, 7 days per week onto a hard disc drive. Images can be recorded onto CD ROM, DVD or hard disk drive.

g. Evidence

The procedure in respect of recordings, which may contain evidence that will be required by the police, is as follows:

Designated police officers will request to view a recording based upon specific time and date parameters. Operators should ensure that all such viewing requests are done so by appointment.

The Operator will view the recording along with the police officer based upon specific start and finish time and date. This viewing is recorded on an internal viewing form.

Should the material to be viewed be relevant to an on-going criminal investigation or specific court case, the police officer will request a copy of the recording. This request is logged onto the Internal Viewing Form.

The relevant material will then be copied by the Operator onto a DVD, CD ROM or hard disk drive provided by the police.

The recording should be clearly marked as evidence and should be released only when it has been signed for on the Evidential Record and the Master Log Sheet of the Evidential file is completed.

Exactly the same procedure is followed in the event of a request from the Police Ombudsman to view any recordings from the System.

h. Provision of Services to the media

Under no circumstances must CCTV Operators contact or speak to the media. (Media includes local radio, television, print journalists or related staff).

Under no circumstances must you make any approaches to the media or discuss anything that you have seen or learnt through your employment as a CCTV Operator at Southampton City Council.

Any dealings with the media should be done in consultation with the Council's Public Relations Department.

i. Emergency procedures

If the need arises to evacuate the Control Room by virtue of either a security alert or fire alarm all staff will act in accordance with local instructions. If possible, and without risking the safety of any member of staff, the room will be secured on leaving. Any operations or procedures underway at the time of the evacuation should be abandoned.

Upon returning to the room all systems should be checked to ensure that they are in proper working order and an appropriate entry should be recorded on the Incident Log.

j. Data Protection Act 1998 – Subject Access Request

The content of the recordings made by the System is 'Data', and as such is covered by the Data Protection Act 1998. People who appear in recordings (Data Subjects) have the legal right to view any material in which they appear. However the right does not extend to some types of incidents or recordings. It is the responsibility of the Data Controller to grant access to recordings and all requests must be directed to the Data Controller in writing.

If an Operator receives a request for access to images from anyone other than a recognised police officer or the CCTV Manager, they must not discuss with them the contents of any recording observation made by the System.

The Data Controller may require Operators to check recordings of specific incidents, but no non-authorised individuals must be present.

Members of the public or others requesting access must be directed to the Council's Information Compliance officer or be directed to the appropriate area on the Council's website.

k. Requests for planned covert observations

If a known individual or group of known individuals is the subject of a request and request comes from a 'public authority' e.g. police, local authority, Customs & Excise then the Regulation of Investigatory Powers Act 2000 may apply.

Unless in 'hot pursuit' of a suspect, which would make obtaining the necessary authority impractical, then all such observation requests must be accompanied by a written authority from an authorising officer. In the case of the police, this will be an officer of the rank of Inspector or above and in the case of Southampton City Council this will be a recognised senior officer through the CCTV Manager. (Please refer to *Southampton City Council Corporate Surveillance Guidance*).

In the event of a major event taking place e.g. political demonstration, sporting event, or other event that is likely to be the source of public disorder, the police may request that a police officer be present in the Control Room for the duration of the event. The officer needs to have written authority signed by a chief inspector or above, which details the duration of the event with specific start and finish times detailed on the form in order to be present in the Control Room. Approval for this will be given only after consultation with the CCTV Manager.

SCHEDULE 3: COMPLAINTS PROCEDURE

We hope to resolve complaints at the earliest opportunity. If this is not possible, our complaints procedure has three stages and at each stage your complaint will be considered by someone different.

Stage 1

If you are unhappy about the service you have received or consider you have been treated unfairly, you can make a complaint. Please fill in a comments, compliments and complaints feedback form which is automatically sent to the relevant service area. You can also make your complaint by phone, email or in writing to

Corporate Complaints Officer
Corporate Policy & Performance Division
Southampton City Council
Civic Centre
Southampton
SO14 7NR

Your complaint will be acknowledged by the appropriate service. An officer within the service will investigate and respond directly to you.

You will receive a full reply within 10 working days

We will consider your complaint closed four weeks after we send the full response letter unless you have asked for the case to be taken to stage 2.

Stage 2

If you are not happy with the response to your complaint and you feel that the problem has not been resolved you can ask that your complaint is investigated by the Head of Service of the area concerned. You will have been given the contact details for the Head of Service in the stage 1 response letter.

You will need to let us know, within 4 weeks of the stage 1 response, which bits of your complaint you feel have not been properly dealt with.

We will take your complaint seriously and respond to you within 20 working days.

Stage 3

If you feel the matter has still not been resolved after stage 2, you may ask that your complaint is investigated at stage 3. This will be investigated by the Corporate Complaints Officer or a senior officer independent of the service area concerned. You need to let us know within four weeks of our contact with you.

To do this, you need to tell us which elements of your complaint you feel we have not properly dealt with and then write to the corporate complaints officer their details are at the bottom of the page.

complaints@southampton.gov.uk

We will take your complaint seriously and respond to you within 20 working days after a full investigation.

Local Government Ombudsman

We aim to resolve your complaint. However if you are not satisfied with our stage 3 response you may contact the Local Government Ombudsman

Local Government Ombudsman

PO Box 4771

Coventry

CV4 0EH

By phone: 0300 061 0614

By email: advice@lgo.org.uk

Website: link to the Local Government Ombudsman is at the bottom of the page

The Local Government Ombudsman will not take up your complaint until the council has had a fair chance to look into the matter first.

Useful contact details

If you wish to make a complaint and are not sure how to contact a Service directly, you can get in touch by contacting Gateway Southampton. Email: gateway@southampton.gov.uk

by post or in person to:

Gateway Southampton

One Guildhall Square

Southampton

SO14 7FP

Link **here** to the on-line Corporate Complaints procedure

APPENDIX A: RELEASE OF DATA TO THIRD PARTIES

Introduction

Arguably CCTV is one of the most powerful tools to be developed during recent years to assist with efforts to combat crime and disorder whilst enhancing community safety. Equally, it may be regarded by some as the most potent infringement of people's liberty. If users, owners and managers of such systems are to command the respect and support of the general public, the systems must not only be used with the utmost probity at all times, they must be used in a manner which stands up to scrutiny and is accountable to the very people they are aiming to protect. It should be noted that the release of the requested data remains at the discretion of Southampton City Council.

General policy

Requests for the release of data are to be passed to the Corporate Legal Team. The Information Compliance officer (on behalf of the Council) can refuse an individual request to view footage, if insufficient or inaccurate information is provided. A search request should specify reasonable accuracy i.e. within 15 minutes.

Primary request to view data for evidential purposes

a) Primary requests to view data generated by a CCTV System are likely to be made by third parties for any one or more of the following purposes:

- i) providing evidence in criminal proceedings (e.g. police and Criminal Evidence Act 1984, Criminal Procedures & Investigations Act 1996, etc.);
- ii) providing evidence in civil proceedings or tribunals;
- iii) the prevention of crime;
- iv) the investigation and detection of crime (may include identification of offenders) ;
- v) identification of witnesses.

b) Third parties, who 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, (e.g. Customs and Excise; Trading Standards);
- iii) solicitors;
- iv) plaintiffs in civil proceedings;
- v) accused persons or defendants in criminal proceedings;
- vi) other agencies specified in the Code.

c) Upon receipt from a third party of a bona fide request for the release of data, the Council will:

- 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.

d) In circumstances outlined at note (3) below, (requests by plaintiffs, accused persons or defendants) the Council will:

- i) be satisfied that there is no connection with any existing data held by the police in connection with the same investigation;
- ii) treat all such enquiries with strict confidentiality.

Secondary request to view data.

A 'secondary' request for access to data may be identified as any request being made which does not fall into the category of a 'primary' request. Before complying with a secondary request, the Council shall ensure that the request does not contravene, and that compliance with the request would not breach, current relevant legislation (e.g. Data Protection Act 1998, Human Rights Act 1998, Criminal Justice and Public Order Act, Freedom of Information Act 2000 etc.);

If, in compliance with a secondary request to view data, a decision is taken to release material to a third party under the auspices of 'crime and prevention', written agreement to the release of the material should be obtained from a police officer, not below the rank of Inspector. The officer should have personal knowledge of the circumstances of the crime/s to be prevented and an understanding of the Code.

Making a Subject Access Request

a) Under the terms of Data Protection Act 1998 (section 7), individual access to personal data, of which an individual is the Data Subject, must be permitted providing:

- i) the request is made in writing (see Appendix C);
- ii) the specified fee is paid for each individual search;
- iii) the Council is supplied with sufficient information to satisfy him or her self 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 information which that person seeks to be located;
- v) the person making the request is only shown information relevant to that particular search and which contains personal data of her or him self only, unless all other individuals who may be identified from the same information have consented to the disclosure.

b) In the event of the Council complying with a request to supply a copy of the data to the subject, only data pertaining to the individual will be copied, (all other personal data which may facilitate the identification of any other person should be concealed or erased);

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

Process of disclosure:

a) Verify the accuracy of the request;

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

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

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

APPENDIX B: DECLARATION OF CONFIDENTIALITY

The Southampton City Council CCTV system Declaration of Confidentiality

I _____ am retained by _____ to perform the duty of CCTV Control Room Operator on behalf of Southampton City Council. I have received a copy of the CCTV Code of Practice in respect of the Operation and management of the System.

I hereby declare that:

I am fully conversant with the content of the Code and understand that all the duties which I undertake in connection with the System must not contravene any part of the Code, or any future amendments of which I am 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, 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 System, verbally, in writing or by any other media, now or in the future.

In appending my signature to this declaration, I agree to abide by the Code at all times, I also understand and agree to maintain confidentiality in respect of all information gained during the course of my duties whether received verbally, in writing or any other media format now or in the future.

Signed: _____

Print name: _____

Witness: _____

Position: _____

Dated this _____ day of _____ (month) 20 _____

APPENDIX C: SUBJECT ACCESS FORM

How to apply for information held on Southampton City Council's CCTV System

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

Your rights

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

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

Southampton City Council's rights

Southampton City Council may deny access to information where the Data Protection Act 1998 allows. The main exemptions in relation to information held on the CCTV system are where the information may be held for:

- prevention and detection of crime; and/or
- apprehension and prosecution of offenders and giving you the information may be likely to prejudice any of these purposes.

Fees

A fee of £10 is payable for each Subject Access Request, which must be in pounds sterling. Cheques and Postal Orders should be made payable to 'Southampton City Council'.

There is a link [here](#) to the Subject Access Request for CCTV application form.