

# Portsmouth City Council

Code of Practice  
For the operation of  
Closed Circuit Television  
Based upon



Model Documents

August 2014



Portsmouth  
CITY COUNCIL

Code of Practice  
in Respect of the Operation of  
**Portsmouth City Council**  
CCTV System

## **Contents**

## **Section**

|   |            |
|---|------------|
| Introduction and Objectives                   | Section 1  |
| Statement of Purpose and Principles           | Section 2  |
| Privacy and Data Protection                   | Section 3  |
| Accountability and Public Information         | Section 4  |
| Assessment of the System and Code of Practice | Section 5  |
| Human Resources                               | Section 6  |
| Control and Operation of Cameras              | Section 7  |
| Access to, and Security of Control Room       | Section 8  |
| Management of Recorded Material               | Section 9  |
| Video Prints                                  | Section 10 |

## **Appendices**

|   |            |
|---|------------|
| Key Personnel   | Appendix A |
| Extracts from Data Protection Act 1998                        | Appendix B |
| National Standard for releasing data to third parties         | Appendix C |
| Declaration of Confidentiality for Staff                      | Appendix D |
| Declaration of Confidentiality for Visitors                   | Appendix E |
| Subject Access Request Forms                                  | Appendix F |
| Regulation of Investigatory Powers Act Guidance to CCTV Users | Appendix G |

# Section 1 Introduction and Objectives

## 1.1 Introduction

This Code of Practice has been written under consultation to ensure that the principles, which will govern the regulation and operation of the Portsmouth CCTV System, are known to all staff involved in the operation and all residents of Portsmouth.

Portsmouth City Council has introduced a Closed Circuit Television (CCTV) system into the city as one of an integrated package of measures to reduce crime levels – a positive response to MORI Poll Survey of City Residents. The aim of these measures is to make Portsmouth a safer place for residents, businesses and visitors. All cameras within the system are overt with clear signage and Portsmouth City Council will not install "Dummy" cameras.

This system, known as the Portsmouth City Council CCTV System, comprises of a number of cameras installed at strategic locations. They have been phased in over a number of years since 1996. Most of the cameras are fully operational with pan, tilt and zoom functions. Others are fixed cameras, images from which are present in the same room. Secondary monitoring facilities are located at the Traffic Management Centre Civic Offices, and the Seafront Management Office, Avenue De Caen Southsea. Cascades Shopping Centre, Portsmouth Football Club and Fratton Police Station are also able to monitor some Cameras.

The Main Control Room (MCR) is located in the Civic Offices. This is managed by Portsmouth City Council, with the operation contracted out. It is staffed 24 hours a day, 365 days a year with at least one operator present at all times.

The Traffic Management Centre is situated in the Civic Offices and has use of the systems cameras on request. The sole purpose is to enable the Engineering and Design Services and Traffic Group to view and monitor images to assist in Traffic Management.

The Seafront Management office has use of the cameras for specific events hosted in Southsea. The cameras are controlled from this location by Portsmouth City Council employees.

A Control room exists at Cascades Shopping Centre, which monitors and controls ten cameras from the PCC Surveillance System.

Portsmouth Football Club has facilities to monitor cameras from the system purely on match days. This is at the request of the match commander and is operated by a member of the MCR staff.

Fratton Police station has the facilities to monitor cameras from the System. This Control Room is only operational when a major event is planned.

All secondary monitoring stations are governed by an Operational Protocol signed by a member of each organisation and Portsmouth City Council.

Two additional monitors are installed at the Hampshire Constabulary Control Centre Netley. Only the MCR have recording facilities for the system.

Additionally Portsmouth City Council has invested in a number of rapid deployable cameras, which will be used in Anti-Social Behaviour areas when all other options have been exhausted. The deployment of these cameras will be in accordance with a policy drawn up by a board of members from all partner agencies including Hampshire Constabulary.

## **1.2 Ownership**

For the purpose of this document the “owner” of the system is Portsmouth City Council

The “System Manager” is: - Portsmouth City Council

The “Data Controller” is the CCTV Operations Manager

The Portsmouth City Council system has been notified to the Information Commissioner.

## **1.3 Objectives of the scheme**

The objectives of the Portsmouth City Council system which form the lawful basis for the processing of data are:-

- Reducing the fear of crime, promoting community safety and stimulating continuing economic growth within the community
- Encouraging the use of public and commercial facilities within the City and assisting in the maintenance of public order and reducing offences involving vandalism and nuisance.
- Assisting in the reduction, prevention and detection of crime.
- Providing high quality evidence, which may be used by the Police, Customs and Excise Officers, British Transport Police and Military Police to prosecute offenders and by officers of Portsmouth City Council to assist in carrying out their appointed duties.
- Monitoring road traffic circulation and improving road safety.
- Protecting property.
- Public health and safety

## **1.4 Procedural Manual**

This Code of Practice (hereafter referred to as 'The Code') will be supplemented by a separate procedural manual, which offers detailed operating instructions on the day to day running of the system. To ensure the aims and objectives (see section 2) of the CCTV System are realised, the procedural manual is based upon the contents of this code.

## **Section 2 Statement of Purpose and Principles**

### **2.1 Purpose**

The purpose of this document is to state the intention of the system owner and the process adopted in determining the reasons for implementing the system as the defined objectives in section 1.

### **2.2 General Principles of Operation**

- 2.2.1 The system will be operated fairly, within the law, and only for the purposes for which it was established or which it is subsequently agreed in accordance with this Code.
- 2.2.2 The operation of the system will be in accordance with all the requirements and the 8 Principles of the Data Protection Act.
- 2.2.3 The System will be operated with due regard to the rights of the individual. Particular attention will be paid to the intent of current legislation including the Humans Rights Act 1998 and the Regulation of Investigatory Powers Act 2000.
- 2.2.4 The public interest in the operation of The System will be recognised by ensuring the security and integrity of operational procedures.
- 2.2.5 Throughout this Code it is intended, as far as reasonably possible, to balance the objectives of the System with the need to safeguard individual rights. Every effort has been made throughout the Code to indicate that a formal structure has been put in place, including a complaints procedure, by which it can be identified that the System is not only accountable, but is seen to be accountable.

2.2.6 All participation in The System by any organisation, authority or individual assumes an agreement by all such parties to comply fully with this Code and to be accountable under the Code of Practice.

## **2.3 Copyright**

Copyright and ownership of all material recorded by virtue of The System will remain with Portsmouth City Council.

## **2.4 Monitoring and Recording Facilities**

2.4.1 A staffed monitoring room is located at the Civic Offices, Guildhall Square, Portsmouth. The CCTV equipment has the capability of recording all cameras simultaneously throughout every 24 hour period.

2.4.2 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 in accordance with the Code. All viewing and recording equipment shall only be operated by authorised and trained users and shall only take place within the Control Room.

## **2.5 Human Resources**

2.5.1 The Control Room operation is staffed under contract to a specialised security company and all personnel are screened to BS 7858:2012 and trained in accordance with the Security Industry Authority and hold a valid SIA CCTV Frontline License

2.5.2 All staff and management shall receive training relevant to their role in the requirements of current legislation and the Codes of Practice and Procedure Manual. Ongoing training will be available as necessary.

## **2.6 Operators Instructions**

2.6.1 Technical instructions on the use of the equipment housed in the Control Room are contained in a separate manual.

## **2.7 Processing and Handling of Recorded Material**

2.7.1 All recorded material, whether recorded digitally, in analogue format or as a hard copy video print, will be processed and handled strictly in accordance with this Code and the Procedural Manual.

## **2.8 Changes to the Code or the Procedural Manual**

2.8.1 Any major changes to either the Code or the Procedural Manual, (i.e. such as will have a significant impact on the operation of the system) will take place only after consultation with, and upon the agreement of all organisations with a participatory role in the operation of the system. Unless the change is required by law at which time no consultation will be made.

2.8.2 Any minor changes (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 owner of the system.

## **Section 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 information, (or data) i.e. what happens to the material that is obtained.

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

- I. Organisation, adaptation or alteration of the information or data;
- II. Retrieval, consultation or use of the information or data;
- III. Disclosure of the information or data by transmission, dissemination or otherwise making available, or
- IV. Alignment, combination, blocking, erasure or destruction of the information or data.

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 total respect 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 and additional locally agreed procedures.

### **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. The registration is included in Portsmouth City Council's general registration and is renewed annually.

3.2.2 The Portsmouth City Council CCTV System and other City Council departments, who operate CCTV, for example Housing Service, are notified with the Data Protection Commissioner, as one identity.

3.2.3 All data will be processed in accordance with the eight principles of the Data Protection Act 1998, which, in summarised form includes, but is not limited to:

- I. Personal data shall be processed fairly and lawfully and in particular, shall not be processed unless:
  - a. at least one of the conditions in Schedule 2 is met, and
  - b. in the case of personal sensitive data, at least one of the conditions in Schedule 3 is also met.
- II. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
- III. Personal data will be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- IV. Personal data shall be accurate and where necessary kept up to date
- V. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- VI. Processed in accordance with the rights of data subjects under this act.
- VII. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- VIII. Personal information shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

### **3.3 Requests for Information (Subject Access)**

3.3.1 Any request from an individual for the disclosure of personal data which he/she believes is recorded by virtue of the system will be directed in the first instance to the Data Controller.

- 3.3.2 The principles of Sections 7, 8, 10 and 12 of the Data Protection Act 1998 (right of Data Subjects and others) 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. An appropriate 'Subject Access' request form is included in Appendix F.
- 3.3.5 All requests for information will be dealt with in accordance with the Data Protection Act, CCTV Code of practice and the Portsmouth City Council's CCTV Disclosure Policy and Procedures.

### **3.4 Exemptions to the Provision of Information**

In considering a request made under the provisions of Section 7 of the Data Protection Act 1998, reference may also be made to section 29 of the Act, which includes but is not limited to the following statement:

- 3.4.1 Personal data processed for any of the following purposes -
- a) the prevention or detection of crime
  - b) the apprehension or prosecution of offenders

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

**NB Each and every application will be assessed on its own merits and general 'blanket exemptions' will not be applied.**

### **3.5 Criminal Procedures and Investigations Act 1996**

The Criminal Procedures and Investigation Act came into effect on 1<sup>st</sup> April 1997 and introduced a statutory framework for the disclosure to defendants of material which the

Code of Practice for the **Portsmouth City Council**

Based upon the CCTV User Group Code of Practice © Copyright

prosecution would not intend to use in the presentation of its own case, (known as 'unused material'). An explanation summary of the provisions of the Act is contained within the Procedural manual, but disclosure of unused material under the provision of this Act should not be confused with the obligations placed on the data controller by Section 7 of the Data Protection Act 1998, (known as subject access).

### **3.6 Release of information to the Media**

3.6.1 It is the City Council's policy that information will not be released to the media. The only exceptions are:

- a) A case where the police have not been able to trace or identify a suspect after undertaking normal investigations and where they believe that general disclosure will assist. In such cases, the police will seek the consent of the City Council prior to disclosure and the City Council will wish to be satisfied that the advantages of the disclosure outweigh the prejudicial effect.
  
- b) Where CCTV footage has been used in a court case and a conviction has been obtained, stills of that footage might be released where this would enhance the purpose of the system. Release of stills would be subject to strict conditions.

## **Section 4 Accountability and Public Information**

### **4.1 The Public**

- 4.1.1 For reasons of security and confidentiality, access to the CCTV Control Room is restricted in accordance with this Code. However, in the interest of openness and accountability, anyone wishing to visit the room may be permitted to do so, subject to the approval of, and after making prior arrangements with the data Controller.
- 4.1.2 Cameras will not be used to look into private residential property. Where the system permits 'Privacy zones' will be programmed into the system as required ensuring the interior of any private residential premise within the range of the system will not be viewed by camera. For areas where such 'zones' cannot be programmed, steel plates will be used if available and CCTV Controllers will be 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 Portsmouth City Council. All complaints shall be dealt with in accordance with the Portsmouth City Council's complaints procedure, a copy of which may be obtained from the Civic Offices, Guildhall Square.
- 4.1.4 All CCTV staff are contractually subject to regulations governing confidentiality and discipline.

### **4.2 System Owner**

- 4.2.1 The System is owned by Portsmouth City Council.

### **4.3 Data Controller**

- 4.3.1 The Data Controller, named in Appendix A, being the nominated representative of the system owner, will have unrestricted personal access to the CCTV Control Room and will have day-to-day responsibility for the system as a whole.
- 4.3.2 The Data Controller will ensure that every complaint is acknowledged in writing and dealt with in accordance with Portsmouth City Council's corporate complaints procedure.

### **4.4 Public information**

#### 4.4.1 Code of Practice

A copy of this Code shall be published on the Portsmouth City Council website, and a copy will be made available to anyone on request. Additional copies will be lodged at public libraries throughout the city, at Police Stations within the city and at the Civic Offices, Guildhall Square.

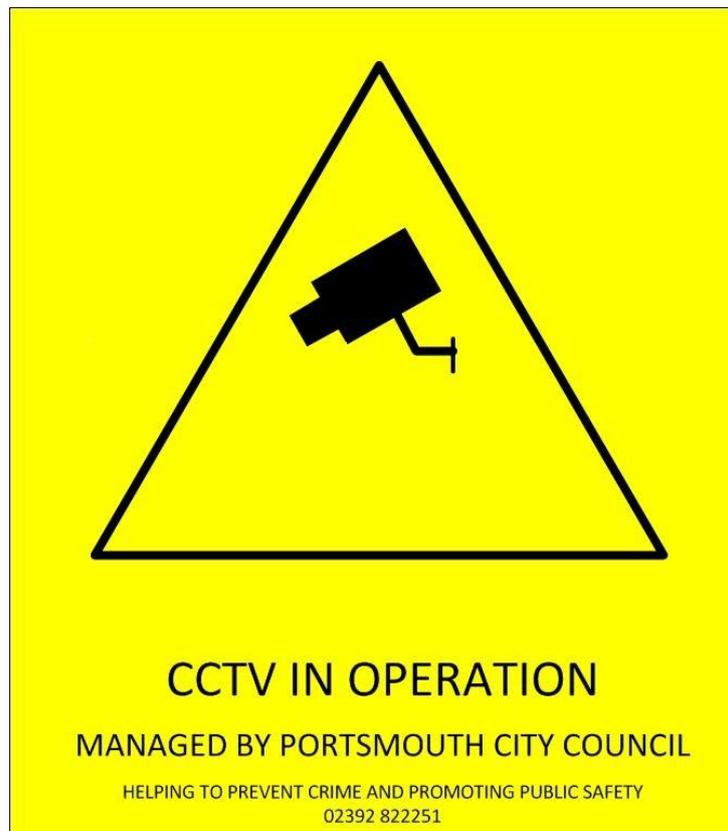
#### 4.4.2 Annual Report

The annual report and that for subsequent years shall be published by the end of June in the year following the report year. A copy of the annual report will also be made available to anyone requesting it. Additional copies will be lodged at public libraries, local police stations and at the Civic Offices, Guildhall Square.

#### 4.4.3 Signs

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

- The presence of CCTV Monitoring
- The 'Ownership' of the system
- Contact telephone number of the 'data controller' of the system



## **Section 5      Assessment of the System and Code of Practice**

### **5.1      Evaluation**

5.1.1      The system will periodically be independently evaluated to establish whether the purposes of the system are being complied with and whether objectives are being achieved. The evaluation will assess the Inputs, the Outputs, the Process and the Impact of the scheme.

- a. An assessment of the impact upon crime
- b. An assessment of the impact on business
- c. An assessment of incidents monitored by the system
- d. The views and opinions of the public
- e. The operation of the Code of Practice
- f. Whether the purposes for which the system was established are still relevant
- g. Cost effectiveness

5.1.2      The results of the evaluation will be published and will have a bearing on the future functions, operations and management of the system.

### **5.2      Monitoring**

5.2.1      The Data Controller will accept day to day responsibility for the monitoring, operation and evaluation of the system and the implications of this Code.

5.2.2      The Data Controller shall also be responsible for maintaining full information for incidents monitored by the Control Room, for use in management of the system and future evaluations.

### **5.3      Audit**

The Data Controller will be responsible for regularly auditing the operation of the system and compliance with this Code. Audits, which may be in the form of irregular spot checks, will include examinations of recorded footage and associated paperwork.

## Section 6

## Human Resources

### 6.1 Staffing of the Control Room

- 6.1.1 It is acknowledged that any CCTV System is only as good as the management of the material being recorded. Only authorised personnel who have been properly trained will handle recorded information, gathered by Portsmouth City Council CCTV Systems. Each person having direct involvement with the System will be given access to a copy of both the Code of Practice and associated Procedural Manual. 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 at all times, and understand that failure to comply would result in disciplinary action.
- 6.1.2 Arrangements may be made for Police, Customs and Excise, British Transport Police, MOD Police or Naval Service Police to be present in the Control Room at certain times, subject to agreed protocols. All operation of the system will still be made by trained authorised personnel.
- 6.1.3 All personnel involved with the system will receive additional training from time to time in relation to legislation appropriate to their role.

### 6.2 Discipline

- 6.2.1 Every individual with any responsibility under the terms of this Code and who has any involvement with the System to which they refer, will be subject to a disciplinary code. Those working for Portsmouth City Council will be subject to that organisations code. All contractor staff will be subject to the code of the security company holding the contract at the time or to the contract agreed between Portsmouth City Council and that company. Any breach of this Code or any aspect of confidentiality will be dealt with by those disciplinary rules.
- 6.2.2 The Data Controller will accept primary responsibility for ensuring there is no breach of security and that this Code is complied with. He has day to day responsibility for the management of the room and for enforcing the discipline rules. Non-compliance with this Code by any person will be considered a severe breach of discipline and dealt with accordingly including, if appropriate, the instigation of criminal proceedings.

### 6.3 Declaration of Confidentiality

Every individual with any responsibility under the terms of this Code and who has any involvement with the System to which they refer, will be required to read and sign a declaration of confidentiality. (See appendix E, see also Section 8 concerning access to the Control Room).

### 6.4 Recruitment and Selection

- 6.4.1 All recruitment and selection will adhere to the policy and procedures of the Contracted Security Company and involve through validation the suitability of the candidate to work in a CCTV Control Room.
- 6.4.2 All Contracted Security Company personnel involved with any part of the operation of the system will be trained to current Security Industry Authority (SIA) standards and will hold a valid Frontline CCTV License.

## **Section 7 Control and Operation of Cameras**

### **7.1 Guiding Principles**

- 7.1.1 Any person operating the cameras will act with the upmost probity at all times.
- 7.1.2 The cameras, control equipment, reviewing and recording equipment shall at all times only be operated by persons who have been trained in their use and all legislative implications of their use. During training on the operational systems, trainees will be under the full supervision of a qualified controller at all times.
- 7.1.3 Every use of the cameras will accord with the purposes and key objectives of the system and shall be in compliance with this Code.
- 7.1.4 Cameras will not be used to look into private residential property. 'Privacy Zones' will be programmed into the system (wherever available), in order to ensure that the interior of any residential property within range cannot be viewed by the cameras.
- 7.1.5 Camera operators shall be mindful of exercising prejudices which may lead to complaints of the system being used for purposes other than those for which it is intended. The operators may be required to justify their interest in or recording of, any particular individual, groups of individuals or property at any time by virtue of the audit of the system or by the Data Controller.

### **7.2 Primary Control**

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

### **7.3 Secondary Control**

Secondary control and monitoring facilities are installed (see section 1.1) but these locations have no recording facility.

### **7.4 Operational Command of the System by the Police**

- 7.4.1 Under extreme and rare 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 event that has a significant impact on public safety or prevention and detection of crime. Such use will provide the Police with an overview of the events in order to command the incident.
- 7.4.2 Such requests will be viewed separately to the use of the systems' cameras with regard to the requirement for an authority for specific types of surveillance under the Regulation of Investigatory Powers Act 2000. See Appendix G.

7.4.3 Only requests made on the written request of a police officer not below the rank of Superintendent will be considered. Any such request will only be accommodated on the personal written authority of the System Manager. 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 Superintendents' written request. The request will contain relevant details including date, time, reason for directed surveillance and a signature of the authorising officer. This form will be kept within the Control Room for a period of five years.

7.4.4 In the event of a request being authorised, 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 Sections 6 and 7 of this Code. They will operate under the command of the authorised Police officer, taking into account their responsibilities under this Code.

## **7.5 Maintenance of the System**

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

7.5.2 The maintenance agreement shall make provision for routine/periodic service checks on all equipment, which will include cleaning of any all-weather housings or camera domes, minor adjustments to settings of all equipment that need to be made to maintain good picture quality.

7.5.3 The maintenance agreement will also include any emergency out of hours callouts that require a CCTV specialist to attend site and rectify any loss of severe degradation of picture quality.

7.5.4 It is the responsibility of the Data Controller to ensure all records are maintained in respect of the functioning of the System and the response of the maintenance organisation.

## **Section 8 Access to, and Security of Control Room**

### **8.1 Authorised Access**

Only authorised and trained personnel will operate any of the equipment associated with the System. Access of the Control Room will be limited to the duty operators, authorised personnel from Portsmouth City Council, Police, authorised maintenance engineers and officers from statutory services. All other visits will need to be arranged and agreed through the Data Controller. A list of authorised personnel will be maintained within the Procedural Manual. An access log will be maintained to detail any person entering the Control Room.

### **8.2 Public Access**

Public access to the Monitoring and recording facility will only be authorised by the Data Controller. Any such visits will be conducted and recorded in accordance with the Procedural Manual.

### **8.3 Authorised Visits**

Visits by inspectors or auditors do not fall into the scope of the above paragraph and may take place at any time, without prior warning, but will still require authorisation of the Data Controller. No more than two inspectors or auditors will visit at any one time. Inspectors or Auditors will not influence any part of the System during their visit. Any such visit will be recorded in the same way as described above.

### **8.4 Declaration of Confidentiality**

All visitors to the Control Room, regardless of their status, including Inspectors and auditors will be required to sign the visitor's book and a declaration of confidentiality and entry is dependent on acceptance of the need for confidentiality. A typical notice is included in Appendix E.

### **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, the provisions of the Procedural Manual will be complied with.

- 8.5.2 The Control Room will at all-time be secured by Mechanical and Electronic locks operated by the duty operators.
- 8.5.3 All visitors, including contractors will be supervised by duty operators during their entire stay.

## Section 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 or by way of video copying, including video prints.
- 9.1.2 Every digital recording used in conjunction with the System has the potential of containing material that has 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 everyday activities by virtue of the System, will be treated with due regard to their individual right to respect for their private and family life.
- 9.1.4 It is therefore, of the utmost importance that every means or format (e.g. Paper copy, CD/DVD, or any form of electronic processing and storage) of images obtained from the System, are treated strictly in accordance with this Code and the Procedural Manual from the moment they are received by the Control Room until final destruction. All movement and usage will be meticulously recorded.
- 9.1.5 Access to and the 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 National standard for the release of data to a third party

- 9.2.1 Every request for the release of data generated by the System will be channelled through the Data Controller. The Data Controller will ensure the principles contained in Appendix C of this Code are followed at all times.
- 9.2.2 In complying with the national standard for the release of data to third parties, it is intended, as far as reasonably practicable, to safeguard the individuals rights to privacy and to give effect to the following principles.
- a) Recorded material shall be processed fairly and lawfully, and used only for the purpose defined in this Code.
  - b) Access to recorded material will take place in accordance with the standards outlined in Appendix C of this Code.
  - c) The release or disclosure of data for commercial or entertainment purposes is strictly 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 appendix C, release details of recorded information to the media only in an effort to identify alleged offenders or potential witnesses.

Under such circumstances, full details will be recorded in accordance with the Procedural Manual.

### **9.3 Digital Recording Equipment**

- 9.3.1 All video information recorded by virtue of the system will be recorded onto Digital Video Recorders (DVR). A daily system check will provide information to the quality and retention of information.
- 9.3.2 All Digital Video Recorders will be maintained in accordance with the Procedural Manual and information obtained will be automatically electronically overwritten in accordance with the Data Protection Act.
- 9.3.3 A log will be maintained for every use of the Digital Recording facilities and will include any viewings and copies of footage and maintenance of the equipment.

### **9.4 Evidential Material**

- 9.4.1 In the event of video footage being required for evidential purposes the procedures outlined in the Procedural Manual will be fully complied with.

### **9.5 Recording Policy**

- 9.5.1 Subject to the equipment functioning correctly, images from every camera will be recorded throughout every 24 hour period in 24 hour time lapse mode, on digital recorders onto digital tapes or computer disk. The number of images through each recorder will be such that the time between successive frames once played back in time lapse mode shall not exceed 2 seconds.
- 9.5.2 Images from selected cameras will be recorded in real time at the discretion of the CCTV controllers or as directed by the System Manager.

## Section 10 Video Prints

### 10.1 Guiding Principles

- 10.1.1 A video print is a copy of an image or images which already exist on video tape / computer disc. Such prints are equally 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 release under the terms of this Code, 'Release of data to third parties'. If prints are release to the media, (in compliance with paragraph 3.6), in an effort to identify alleged offenders or potential witnesses, full details will be recorded in accordance with the Procedural Manual.
- 10.1.3 A record will be maintained of all video print productions in accordance with the Procedural Manual. The recorded details will include;
- a) A sequential number.
  - b) The date.
  - c) Time and location of the incident.
  - d) Date and time of the production of the print.
  - e) Identity of the person requesting the print, (if relevant).
  - f) Signature of the person collecting the print.

## Appendix A

## Key Personnel

### System Owners

Portsmouth City Council  
Civic Offices  
Guildhall Square  
Portsmouth  
PO1 2BY

Tel: 023 9282 2251

### Responsibilities:

Portsmouth City Council is the 'Manager' of the system. The Service Manager will be the initial point of reference on behalf of the Owners, whose role will include a responsibility to:

- a) Ensure the provision and maintenance of all equipment forming part of the Portsmouth City Council System in accordance with contractual arrangements which the owners may from time to time enter into.
- b) Maintain close liaison with the control room operators.
- c) Ensure the interests of the joint owners and other organisations are considered in accordance with the terms of this Code of Practice.
- d) Agree to any proposed alterations and additions, this Code of Practice and / or the Procedural Manual.

### System Management

The person responsible for system management will be:

Anthony Hadley  
CCTV Operations Manager  
Portsmouth City Council  
Civic Offices  
Guildhall Square  
Portsmouth  
PO1 2BY

Tel: 023 9284 1044

Fax: 023 9284 1306

Email: [Anthony.hadley@portsmouthcc.gov.uk](mailto:Anthony.hadley@portsmouthcc.gov.uk)

The System Managers responsibilities will include:

- a) Day to day management of the system and staff;
- b) Overall day to day responsibility for the system and for ensuring that this Code of Practice is complied with;
- c) Maintain direct liaison with the owners of the system.
- d) Maintain direct liaison with operating partners.

Code of Practice for the **Portsmouth City Council**

Based upon the CCTV User Group Code of Practice © Copyright

- e) Be responsible for the daily running of the CCTV system and to liaise with the maintenance contractor to ensure that the system functions as specified
- f) Delegated authority for data controller on behalf of the ‘System Owners’

# Appendix B Extracts from Data Protection Act 1998

## Section 7

- (1) Subject to the following provisions of this section and 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 the data controller,
  - (b) if that is the case, to be given by the data controller a description of -
    - (i) the personal data of which that individual is the data subject
    - (ii) the purpose of which they are being or are to be processed and
    - (iii) the recipient or class of recipients to whom they are or may be disclosed,
  - (c) to have communicated to him in an intelligible form –
    - (i) the information constituting any personal data of which that individual is the data subject, and
    - (ii) any information available to the data controller as to 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 purpose 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 (1) unless he has received –
  - (i) a request in writing, and
  - (ii) 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 reasonably require in order to satisfy himself 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 –
  - (i) the other individual has consented to the disclosure of the information to the person making the request, or
  - (ii) it is reasonable in 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 the 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 with disclosing the identity of the other individual concerned, whether by omission of names or other particulars or otherwise.

- (6) In determining the purpose 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 –
- (i) any duty of confidentiality owed to the other individual,
  - (ii) any steps taken by the data controller with a view to seeking the consent of the other individual,
  - (iii) whether the other individual is capable of giving consent, and
  - (iv) any express refusal of consent by the other individual.
- (7) An individual making a request under this subsection 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 -
- “Prescribed” means prescribed by the Secretary of State by regulations
- “The prescribed maximum” means such amount as may be prescribed
- “The prescribed period” means forty days or such other period as may be prescribed
- “the relevant day”, in relation to a request under this section means the day on which the data controller receives 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.

**Note:** These extracts are for initial direction and guidance only. To ensure compliance with the legislation the relevant Data Protection legislation should be referred to in its entirety.

**Copies of the act and the Information Commissioners code of Practice can be downloaded from their website**

[www.legislation.gov.uk](http://www.legislation.gov.uk)

Code of Practice for the **Portsmouth City Council**

Based upon the CCTV User Group Code of Practice © Copyright

## 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 subsection 7(1)(c)(I) must be complied with by supplying the data subject with a copy of the information in permanent form unless –
  - (i) the supply of such a copy is not possible or would involve disproportionate effort, or
  - (ii) The data subject agrees otherwise:

And where any of the information referred to in subsection 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 the purpose 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 any 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 purpose 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 reasonable belief of the data controller, is likely to be in, or to come into, the possession of the data subject making the request.

**Note:** These extracts are for initial direction and guidance only. To ensure compliance with the legislation the relevant Data Protection legislation should be referred to in its entirety.

**Copies of the act and the Information Commissioners code of Practice can be downloaded from their website**

[www.legislation.gov.uk](http://www.legislation.gov.uk)

Code of Practice for the **Portsmouth City Council**

Based upon the CCTV User Group Code of Practice © Copyright

# APPENDIX C National Standard for releasing data to third parties

## 1. 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.

Portsmouth City Council are committed to the belief that everyone has the right to respect for his or her private and family life and their home. Although the use of CCTV cameras has become widely accepted in the UK as an effective security tool, those people who do express concern tend to do so over the handling of the information (data) which the System gathers.

After considerable research and consultation, the nationally recommended standard of the CCTV User Group has been adopted by the System owners.

## 2. General Policy

All requests for the release of data shall be processed in accordance with the Procedure Manual. All such requests shall be channelled through the data controller.

## 3. Primary Request to View Data

- a) Primary requests to view data generated by a CCTV System are likely to be made by third parties for any one or more of the following purposes:
  - (i) Providing evidence in criminal proceedings (e.g. Police and Criminal Evidence Act 1984, Criminal Procedures & Investigations Act 1996, etc.);
  - (ii) Providing evidence in civil proceedings or tribunals
  - (iii) The prevention of crime
  - (iv) The investigation and detection of crime (may include identification of offenders)
  - (v) Identification of witnesses
  
- b) Third parties, which are required to show adequate grounds for disclosure of data within the above criteria, may include, but are not limited to:
  - (i) Police <sup>(1)</sup>
  - (ii) Statutory authorities with powers to prosecute, (e.g. Local Authority Departments, Customs and Excise; Trading Standards, etc.)
  - (iii) Solicitors <sup>(2)</sup>
  - (iv) Plaintiffs in civil proceedings <sup>(3)</sup>
  - (v) Accused persons or defendants in criminal proceedings <sup>(3)</sup>

- (vi) Other agencies, (which should be specified in the Code of Practice) according to purpose and legal status <sup>(4)</sup>.
- c) 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.
- d) In circumstances outlined at note (3) below, (requests by plaintiffs, accused persons or (defendants) the data controller, or nominated representative, shall:
  - (i) Be satisfied that there is no connection with any existing data held by the police in connection with the same investigation.
  - (ii) Treat all such enquiries with strict confidentiality.

## Notes

- (1) The release of data to the police is not be restricted to the civil police but could include, (for example) British Transport Police, Ministry of Defence Police, Military Police, etc. (It may be appropriate to put in place special arrangements in response to local requirements).
- (2) Aside from criminal investigations, data may be of evidential value in respect of civil proceedings or tribunals. In such cases a solicitor, or authorised representative of the tribunal, is required to give relevant information in writing prior to a search being granted. In the event of a search resulting in a requirement being made for the release of data, such release will only be facilitated on the instructions of a court order or subpoena. A charge may be made for this service to cover costs incurred. In all circumstances data will only be released for lawful and proper purposes.
- (3) There may be occasions when an enquiry by a plaintiff, an accused person, a defendant or a defence solicitor falls outside the terms of disclosure or subject access legislation. An example could be the investigation of an alibi. Such an enquiry may not form part of a prosecution investigation. Defence enquiries could also arise in a case where there appeared to be no recorded evidence in a prosecution investigation.
- (4) The data controller shall decide which (if any) "other agencies" might be permitted access to data. Having identified those 'other agencies', such access to data will only be permitted in compliance with this Standard.
- (5) The data controller can refuse an individual request to view if insufficient or inaccurate information is provided. A search request should specify reasonable accuracy (could be specified to the nearest ½ hour)

## 4. Secondary Request to View Data

- a) A 'secondary' request for access to data may be defined as any request being made which does not fall into the category of a primary request. Before complying with a secondary request, the data controller shall ensure that:
  - (i) 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, 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 1998);
  - (iii) Due regard has been taken of any known case law (current or past) which may be relevant, (e.g. R v Brentwood BC ex p. Peck) and
  - (iv) The request would pass a test of ‘disclosure in the public interest’ <sup>(1)</sup>.
- b) If, in compliance with a secondary request to view data, a decision is taken to release material to a third party, the following safeguards 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 the CCTV System Code of Practice <sup>(2)</sup>.
  - (ii) If the material is to be released under the auspices of ‘public wellbeing, 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 the CCTV System Code of Practice.
- c) Recorded material may be used for bona fide training purposes such as police or staff training. Under no circumstances will recorded material be released for commercial sale of material for training or entertainment purposes.

## Notes

- (1) ‘Disclosure in the public interest’ could include the disclosure of personal data that:
  - (i) provides specific information which would be of value or of interest to the public well being
  - (ii) identifies a public health or safety issue
  - (iii) leads to the prevention of crime
- (2) The disclosure of personal data which is the subject of a ‘live’ criminal investigation would always come under the terms of a primary request, (see III above).

## 5. Individual Subject Access under Data Protection legislation

- a) Under the terms of Data Protection legislation, individual access to personal data, of which that individual is the data subject, must be permitted providing:
  - (i) The request is made in writing;
  - (ii) A specified fee is paid for each individual search;
  - (iii) The data controller 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 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 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 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.
- c) 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.
- d) In addition to the principles contained within the Data Protection legislation, the data controller should be satisfied that the data is:
  - (i) not currently and, as far as can be reasonably ascertained, not likely to become, part of a 'live' criminal investigation;
  - (ii) not currently and, as far as can be reasonably ascertained, not likely to become, relevant to civil proceedings;
  - (iii) not the subject of a complaint or dispute which has not been actioned
  - (iv) the original data and that the audit trail has been maintained;
  - (v) not removed or copied without proper authority;
  - (vi) for individual disclosure only (i.e. to be disclosed to a named subject)

## **6. Process of Disclosure:**

- a) Verify the accuracy of the request.
- b) Replay the data to the requester only, (or responsible person acting on behalf of the person making the request).
- c) The viewing should take place in a separate room and not in the control or monitoring area. Only data which is specific to the search request shall be shown.
- d) It must not be possible to identify any other individual from the information being shown, (any such information will be blanked-out, either by means of electronic screening or manual editing on the monitor screen).
- e) If a copy of the material is requested and there is no on-site means of editing out other personal data, then the material shall be sent to an editing house for processing prior to being sent to the requester.

## **7. Media disclosure**

Set procedures for release of data to a third party should be followed, If the means of editing out other personal data does not exist on-site, measures should include the

- a) In the event of a request from the media for access to recorded material, the procedures outlined under 'secondary request to view data' shall be followed. If material is to be released the following procedures shall be adopted:
  - (i) The release of the material must be accompanied by a signed release document that clearly states what the data will be used for and sets out the limits on its use.
  - (ii) The release form 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.

- (iii) 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).
- (iv) The release form shall be considered a contract and signed by both parties.

## **8. Principles**

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

- a) Recorded material shall be processed lawfully and fairly and used only for the purposes defined in the Code of Practice for the CCTV scheme;
- b) Access to recorded material shall only take place in accordance with this Standard and the Code of Practice;
- c) The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

## **Appendix D Declaration of Confidentiality for Staff**

**You are not to disclose any information involving individuals or groups of individuals, gained while operating or observing the operation of any of the cameras from the CCTV system, to any third party outside the operational staff of the Portsmouth City Council System. Unless in the course of your duties, to one of the following:**

- A. Law Enforcement Agencies where disclosure would assist in a specific criminal enquiry.**
- B. Prosecution agencies**
- C. Relevant legal representatives**

**Or you have the permission of the individual or group of individuals.**

**Or discuss or disclose to any third party, any of the policies or procedures of the CCTV System without the permission of the Data Controller.**

Failure to comply with the above declaration will be a matter to be resolved as part of the City Council's or the contract security companies disciplinary procedures.

## **Appendix E      Declaration of Confidentiality for Visitors**

- 1. This is the Main Control Room for the Portsmouth City Council CCTV System and as such is covered by the Data Protection Act Section 51(3)(b) - Code of Practice for CCTV and the Portsmouth City Council Code of Practice for CCTV, both of which are available for viewing on request. It is also operated with due regard to the rights of the individual and particular attention is paid to current legislation such as the Human Rights Act.**
- 2. As such you are not to disclose to a third party, any information involving individuals or groups of individuals you may gain while visiting this Control Room and viewing the cameras in action.**
- 3. It may also be necessary to suspend your visit and ask you to leave the Control Room immediately, if, in the opinion of the Shift Manager/Senior Operator, it becomes operationally inconvenient.**
- 4. I have read the above document and by signing the Visitors Book, agree to abide by its conditions.**

# Appendix F Subject Access Request Forms

## PORTSMOUTH CITY COUNCIL CCTV SURVEILLANCE SYSTEM

### Data Protection Act, 1998

#### How to Apply For Access To Information Held On the 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. Portsmouth 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)

#### The Council's Rights

Portsmouth City Council may deny access to information where the Act 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
- Apprehension and prosecution of offenders

And giving you the information may be likely to prejudice any of these purposes.

#### Fee

A fee of £10 is payable for each access request, which must be in pounds sterling. Cheques, Postal Orders, etc. should be made payable to 'Portsmouth City Council'.

#### THE APPLICATION FORM: (N.B. ALL sections of the form must be completed. Failure to do so may delay your application.)

**Section 1** Asks you to give information about yourself that will help the Council to confirm your identity. The Council has a duty to ensure that information it holds is secure and it must be satisfied that you are who you say you are.

**Section 2** Asks you to provide evidence of your identity by producing TWO official documents (which between them clearly show your name, date of birth and current address) together with a recent full face photograph of you.

**Section 3** Asks you to confirm whether you will accept just viewing the information, or if you want a copy of the information.

**Section 4** **You must sign the declaration**

When you have completed and checked this form, take or send it together with the required TWO identification documents, photograph and fee to:

**THE CCTV MANAGER, Portsmouth City Council**  
**Civic Offices, Guildhall Square, Portsmouth, PO1 2BY**  
(Receptionist – please complete 'Official Use' Section on page 5.)

**If you have any queries regarding this form, or your application, please ring the CCTV Manager on 023 9284 1044**

**PORTSMOUTH CITY COUNCIL CCTV SURVEILLANCE SYSTEM**  
**Data Protection Act 1998**

**SECTION 1 About Yourself**

*The information requested below is to help the Council (a) satisfy itself as to your identity and (b) find any data held about you.*

**PLEASE USE BLOCK LETTERS**

|   |               |                          |            |                          |               |                          |           |                          |
|---|---------------|--------------------------|------------|--------------------------|---------------|--------------------------|-----------|--------------------------|
| <i>Title (tick box as appropriate)</i>    | <b>Mr</b>     | <input type="checkbox"/> | <b>Mrs</b> | <input type="checkbox"/> | <b>Miss</b>   | <input type="checkbox"/> | <b>Ms</b> | <input type="checkbox"/> |
| <i>Other title (e.g. Dr., Rev., etc.)</i> |               |                          |            |                          |               |                          |           |                          |
| <i>Surname/family name</i>                |               |                          |            |                          |               |                          |           |                          |
| <i>First names</i>                        |               |                          |            |                          |               |                          |           |                          |
| <i>Maiden name/former names</i>           |               |                          |            |                          |               |                          |           |                          |
| <b>Sex (tick box)</b>                     | <b>Male</b>   |                          |            | <input type="checkbox"/> | <b>Female</b> |                          |           | <input type="checkbox"/> |
| <i>Height</i>                             |               |                          |            |                          |               |                          |           |                          |
| <i>Date of Birth</i>                      |               |                          |            |                          |               |                          |           |                          |
| <i>Place of Birth</i>                     | <b>Town</b>   |                          |            |                          |               |                          |           |                          |
|   | <b>County</b> |                          |            |                          |               |                          |           |                          |

|   |                 |  |  |  |  |  |  |  |
|---|-----------------|--|--|--|--|--|--|--|
| <i>Your Current Home Address (to which we will reply)</i>                   |                 |  |  |  |  |  |  |  |
|   |                 |  |  |  |  |  |  |  |
|   | <b>PostCode</b> |  |  |  |  |  |  |  |
| <i>A telephone number will be helpful in case you need to be contacted.</i> | <b>Tel. No.</b> |  |  |  |  |  |  |  |

If you have lived at the above address for less than 10 years, please give your previous addresses for the period:

|                             |              |  |  |                          |            |  |  |                          |
|-----------------------------|--------------|--|--|--------------------------|------------|--|--|--------------------------|
| <i>Previous address(es)</i> |              |  |  |                          |            |  |  |                          |
|                             |              |  |  |                          |            |  |  |                          |
| <b>Dates of occupancy</b>   | <b>From:</b> |  |  | <input type="checkbox"/> | <b>To:</b> |  |  | <input type="checkbox"/> |
|                             |              |  |  |                          |            |  |  |                          |
| <b>Dates of occupancy</b>   | <b>From:</b> |  |  | <input type="checkbox"/> | <b>To:</b> |  |  | <input type="checkbox"/> |

**PORTSMOUTH CITY COUNCIL CCTV SURVEILLANCE SYSTEM**  
**Data Protection Act, 1998**

**SECTION 2 Proof of Identity**

**To help establish your identity your application must be accompanied by TWO official documents that between them clearly show your name, date of birth and current address.**

**For example: a birth/adoption certificate, driving licence, medical card, passport or other official document that shows your name and address.**

**Also a recent, full face photograph of yourself.**

**Failure to provide this proof of identity may delay your application.**

**SECTION 3 Supply of Information**

**You have a right, subject to certain exceptions, to receive a copy of the information in a permanent form. Do you wish to:**

**(a) View the information and receive a permanent copy**

YES / NO

**(b) Only view the information**

YES / NO

**SECTION 4 Declaration**

**DECLARATION (to be signed by the applicant)**

**The information that I have supplied in this application is correct and I am the person to whom it relates.**

**Signed by**

**Date**

**Warning – a person who impersonates or attempts to impersonate another may be guilty of an offence.**

**NOW – please complete Section 4 and then check the ‘CHECK’ box (on page 5) before returning the form.**

**PORTSMOUTH CITY COUNCIL CCTV SURVEILLANCE SYSTEM**  
**Data Protection Act, 1998**

**SECTION 4 To Help us Find the Information**

*If the information you have requested refers to a specific offence or incident, please complete this Section.*

*Please complete a separate box in respect of different categories/incidents/involvement. Continue on a separate sheet, in the same way, if necessary.*

*If the information you require relates to a vehicle, property, or other type of information, please complete the relevant section overleaf.*

Were you:(tick box below)

*A person reporting an offence or incident*

*A witness to an offence or incident*

*A victim of an offence*

*A person accused or convicted of an offence*

**Other – please explain**

|  |  |
|--|--|
|  |  |
|  |  |
|  |  |

**Date(s) and time(s) of incident**

**Place incident happened**

**Brief details of incident**

|  |  |
|--|--|
|  |  |
|  |  |

**PORTSMOUTH CITY COUNCIL CCTV SURVEILLANCE SYSTEM**  
**Data Protection Act, 1998**

|                                   |  |
|-----------------------------------|--|
| <i>Before returning this form</i> | <ul style="list-style-type: none"><li>• <b>Have you completed ALL Sections in this form?</b></li></ul>   |
| <i>Please check:</i>              | <ul style="list-style-type: none"><li>• <b>Have you enclosed TWO identification documents?</b></li><li>• <b>Have you signed and dated the form?</b></li><li>• <b>Have you enclosed the £10.00 (ten pound) fee?</b></li></ul> |

**Further Information:**

These notes are only a guide. The law is set out in the Data Protection Act, 1998, obtainable from The Stationery Office. Further information and advice may be obtained from:

The Information Commissioner,  
Wycliffe House,  
Water Lane,  
Wilmslow,  
Cheshire,  
SK9 5AF.  
Tel. (01625) 545745

Please note that this application for access to information must be made direct to Portsmouth City Council (address on Page 1) and NOT to the Data Protection Commissioner.

**OFFICIAL USE ONLY**

Please complete ALL of this Section (refer to 'CHECK' box above).

**Application checked and legible?**

**Date Application Received**

**Identification documents checked**

**Fee Paid**

**Details of 2 Documents** (see page 3)

**Method of Payment**

**Receipt No.**

**Documents Returned?**

Member of Staff completing this Section:

**Name**

**Location**

**Signature**

**Date**

# Appendix G Regulation of Investigatory Powers Act Guidance to CCTV Users

## Introduction

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

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

## Background

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

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

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

The Act is divided into five parts. Part II is the relevant part of the act for CCTV. It creates a system of authorisations for various types of covert surveillance. The types of activity covered are "intrusive surveillance" and "directed surveillance".

### "Covert surveillance" defined

Observations which are carried out by, or with, the use of a surveillance device. Surveillance will be covert where it is carried out in a manner calculated to ensure that the person or persons subject to the surveillance are **unaware that it is, or may be**, taking place.

## **Part II - Surveillance types**

We should clearly differentiate in this guidance between “Intrusive” surveillance which will be a great rarity for CCTV operations and “Directed” surveillance which will be more likely.

### **“Intrusive” surveillance**

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

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

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

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

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

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

Cameras will not be used to look into private residential property. Where the equipment permits it 'Privacy zones' will be programmed into the system as required 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 controllers will be specifically trained in privacy issues.

### **“Directed” surveillance**

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

The act says:

"Directed surveillance" is defined in subsection (2) as **covert surveillance** that is undertaken in relation to **a specific investigation or a specific operation**

Which is likely to result in the obtaining of **private information** about a person (whether or not one specifically identified for the purposes of the investigation or operation);

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

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

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

If users are requested to operate their cameras as part of a planned operation where the subject is unaware that targeted surveillance is, or may be, taking place; "private information" is to be gained and it involves systematic surveillance of an individual/s (whether or not the target of the operation) then a RIPA "directed surveillance" authority must be obtained.

## **Authorisations**

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

Those who can authorise covert surveillance for public authorities listed in Sch. 1/Part1, in respect to Directed surveillance are detailed in Article 2 / Part I - Statutory Instrument 2417/2000: The Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) Order 2000.

E.g.:

A Local Authority (within the meaning of section 1 of the Local Government Act 1999). The prescribed office as a minimum level of authority is:

Assistant Chief Officer; Officer responsible for the management of an investigation.

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

The impact for staff in Police control rooms and CCTV monitoring centres, is that there might be cause to monitor for some time, a person or premises using the cameras. In most cases, this will be an immediate response to events or circumstances. In this case, it would not require authorisation unless it were to continue for some time. The RIPA draft Code of Practice suggests some hours rather than minutes.

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

The ‘authority’ must indicate the reasons and should fall within one of the following categories:-  
An authorisation is necessary on grounds falling within this subsection if it is necessary-

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

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

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

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

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

## **Policing examples**

### **Insp. Authorisation- urgent request (up to 72hrs)**

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

### **Supt Authorisation – non-urgent request**

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

### **No authorisation required**

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

For access to all relevant information on this Act, including the Schedules and Statutory Instruments referred to in this guidance please visit:

**[www.legislation.gov.uk](http://www.legislation.gov.uk)**

Code of Practice for the **Portsmouth City Council**

Based upon the CCTV User Group Code of Practice © Copyright