

The City of Westminster Closed Circuit Television CCTV

Corporate Code of Practice

Version	Date
V1.7 (WiFi)	December 2005
V1.9 (3)	April 2006



CONTENTS

	Page No
Contents	ii
Certificate of Agreement	iii

Sections

1. Introduction and Objectives	3
2. The System	8
3. Accountability and Public Information	12
4. Assessment of the System and the Code of Practice	14
5. Staffing and Operation of the Control Room	16
6. Control Room Security	18
7. Handling of Recorded Material	19
8. Data Protection, Human Rights and Privacy	21
9. Data Subject Access Requests	23
10. CCTV Copy Prints	25

Attachments

Request for video viewing / extract of data form

1. INTRODUCTION AND OBJECTIVES

Introduction

1.1. This Code of Practice explains the purpose, use, management and monitoring of the various CCTV Systems that are currently deployed and in operation around Westminster (hereinafter referred to as the **System**).

1.2. CCTV Systems means all operations that utilise camera technology irrespective of its means of transmission or mode of image storage

1.3. This Code of Practice is therefore applicable to and used for all CCTV Systems whether fixed or moveable (including re-deployable). This currently includes:

1.3.1. the Westminster CCTV Trust 'Fixed' CCTV System, monitored from the CCTV Control Room at the Trocadero,

1.3.2. the vehicle-based CCTV systems,

1.3.3. the re-deployable (GSM) camera units (OCTV) and

1.3.4. WiFi enabled cameras deployed by Westminster City Council (WCC) as part of a pilot project.

1.4. It also explains how the public can request to view Recorded Material or complain about how the System is managed.

Objectives of the System

1.5. The objectives of the System are to:

- i) provide a tool by which the permitted or authorised 'users' may better and more efficiently undertake their departmental, business unit or contractual responsibilities for the City Council
- ii) assist in the detection, prevention and deterrence of crime and disorder in the area this will include:
 - countering terrorism,
 - helping to identify, apprehend and prosecute offenders,
 - provide the police, other agencies and the City Council with evidence to take criminal and civil action in the courts,
- iii) provide a reduction in the fear of crime and provide reassurance to the public
- iv) increase public safety for those people who live, work, trade and visit Westminster
- v) assist in the overall management of the public space
- vi) assist the City Council in its enforcement and regulatory functions within the area of coverage.
- vii) assist members of the public, businesses or professional individuals with their requests for the appropriate or permitted

information pertaining to incidents that may occur within the area of coverage

Principles of the Code

1.6. The principles of the Code are:

- i) To ensure that the System is operated fairly, impartially and within the law
- ii) To ensure that the System is operated in accordance with the objectives defined in this Code of Practice
- iii) To protect and respect the rights of all individuals who may be filmed
- iv) To offer a balance between the objectives of the System and the need to safeguard the individual's right to privacy, as provided by Article 8 of Schedule 1 to the Human Rights Act 1998, which states that everyone has the right to respect for their private and family life.
- v) To ensure that anyone who makes use of the system should comply fully with and to be accountable under this Code of Practice.
- vi) To ensure that anyone who makes use of the system should be aware of the legislative requirements such as the Data Protection Act 1998 (DPA) or the Freedom of Information Act (FoI) and comply fully with and be accountable under such legislation

Standard Operating Procedural Manual

1.7. This Code is supplemented by separate Standard Operating Procedural Manuals (**SOP's**) for the fixed System, the vehicle based Systems, the re-deployable or WiFi transmitted systems, which offer instructions on all aspects of the operation of those individual System applications. The individual user SOP manual is based upon the contents of this Code of Practice.

Changes to the Code or the Standard Operating Procedural Manual

1.8. Any major changes to either the Code or the SOP's will take place only after consultation with all relevant interested groups, and upon the agreement of all organisations with a participatory role in the operation of the System. A minor change, (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.

Copy of the Code

1.9. A copy of this Code of Practice is available on-line internally on The Wire and externally on the Westminster website.

Whistle blowing procedure

1.10. The System Operator operates a whistle blowing procedure which ensures that staff are encouraged to report breaches to this code in strict confidence through the Human Resources Department

Definitions

1.11. The following offers an explanation for some of the frequently used terms and titles used within this Code and the SOP

1.11.1. The **System** Comprises

- i) the CCTV cameras and their individual mountings
- ii) the image processors and real time monitors
- iii) the time lapse and real time recording and playing equipment
- iv) the computer operating and storage systems (Servers)
- v) the transmission equipment
- vi) the mode of transmission – direct cable or wireless

1.11.2. Reference to the System in this Code applies equally to the following individual applications:

- i) the **'Fixed' CCTV System**, operated by the Westminster CCTV Trust and monitored from the CCTV Control Room at the Trocadero – these cameras are either building or column mounted and linked over a fibre optic or similar third party transmission link directly to the CCTV Control Room.
- ii) the **vehicle-based CCTV systems** – which are stand-alone camera systems mounted on a vehicle with on-board monitoring, control and record/play-back facilities
- iii) the **re-deployable (GSM) camera units (OCTV)** - which are self-contained camera units temporally deployed on appropriate lamp columns which are linked by wireless i.e. over the mobile telephone (GSM) network to a dedicated remote monitoring unit. The camera unit may also include an integrated digital recording unit, which can similarly be integrated remotely via the mobile telephone network.
- iv) the **WiFi enabled cameras** deployed by Westminster City Council as part of an initial pilot project – are similar to the OCTV units in that they are stand-alone units temporally attached to lamp columns. The WiFi units transmit their images and receive their control instructions again by wireless to a nearby wireless node from where the signals are sent over third party data lines to a computer server within the Westminster City Council internal network (intranet). This server is the recording

or archiving media for this system and also the distribution hub for distributing the images and control functions to approved monitoring stations on the network.

1.11.3. **Data Controller** for the purposes of the Data Protection Act 1998 is Westminster City Council. The Data Controller determines the purpose for which, and the manner in which any personal data are, or are to be, processed.

1.11.4. The **Data Processor** is the person or company who processes personal data on behalf of the Data Controller.

1.11.5. All recorded material (images) will be classified as **Data**

1.11.6. The **Owner** of the System has overall responsibility for its operation.

- i) *The 'fixed' CCTV cameras (with the exception of the "LBI" Bus Lane Enforcement Cameras), vehicle based cameras and the OCTV units are under the 'ownership of the Director of Community Protection*
- ii) *The WiFi cameras are under the ownership of the Chief Executive*
- iii) *The LBI Bus Lane Enforcement Cameras are under the ownership of the Director of Parking.*

1.11.7. The **System Manager** is the person responsible for the System as a whole. The System Manager may appoint a deputy.

1.11.8. The **System Administrator** is the person responsible for the administration of that part of the System that relates to Computer Servers and their access protocols. The System Administrator will also be known as the **Data Processor**

1.11.9. The **System Operator** will be appointed by the System Owner to operate the system and will be directly responsible to the System Manager. The System Operator will also be known as the **Data Processor**

1.11.10. The **CCTV Operator** is the duty operator who is trained to operate the System equipment.

1.11.11..The **System Auditor (and nominated deputy)** is responsible for providing an account of the operation of the scheme and Code and SOP, which tests compliance and is the basis of recommendations for good practice.

1.11.12. **Recorded or Archive Material** means any material recorded to 'archive' by, or as the result of, technical equipment, which forms part of the System, but specifically includes images recorded on videotape, digital formats including DVD, CD or computer integral disc or by way of copying onto similar formats including still prints.

1.11.13. **Personal Data** means data, which relates to a living individual who can be identified from those data, either on its own or with other information, which is in the possession of, or is likely to come into the possession of, the Data Controller.

1.11.14. **Processing** has the same meaning as that defined in the Data Protection Act 1998, namely:

Obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

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

1.11.15. **The RIPA Code** is the WCC Code of Practice to the Regulation of Investigatory Powers Act 2000, which regulates the use of covert surveillance. Copies of the RIPA Code are also available to the public (see 1.9 above)

1.11.16. Reference to the **CCTV Control Room** means the control room located within the Trocadero, Piccadilly Circus.

1.11.17. Reference to a **Satellite Monitoring Station** means a secondary monitoring or a viewing location that is not within the CCTV Control Room

1.11.18. Reference to the **vehicle-based CCTV** unit also includes the monitoring or control function integral to that vehicle

2. THE SYSTEM

Cameras and Area of Coverage

2.1. Cameras are placed at various locations in the City of Westminster. The majority of installations are for cameras linked to a cabled transmission service from 'fixed' positions.

2.1.1. The 'fixed' CCTV cameras are mainly distributed around the 'West End' – Oxford Street, Regent Street, Piccadilly, Leicester Square, Soho, China Town, Trafalgar Square and Covent Garden. Additionally there are Housing Estate cameras at Avenue Gardens and within Orange Park as well as the street cameras around Church Street.

i) Additional 'fixed' CCTV cameras have been installed under the remit of the London Bus Initiative (LBI) Bus Lane Enforcement project. These CCTV cameras will be accessible to the Trocadero operators but will also have their own team of specialist enforcement operators in a separate control room.

2.1.2. The vehicle-based CCTV systems are deployed as appropriate around the City following senior officer 'tasking'

2.1.3. The OCTV (GSM) re-deployable units are similarly located for limited periods of times around the City, attached to appropriate lamp-columns following specific senior officer 'tasking'

2.1.4. The WiFi enabled camera units are initially to be located in and around Soho (20 units), Lisson Green Estate (10 units) and Churchill Gardens Estate (10 units).

2.2. The transmitted images are recorded in various formats:- digital format on computer hard discs or DVDs / CDs / mini DVs and also in analogue format on video tape (VHS or SVHS) .

2.3. Most of the cameras have a remote control capability and are classed as fully operational with Pan / Tilt / Zoom facilities whilst a few are of the 'static' type in that they cannot be remotely manoeuvred or controlled.

2.4. Cameras shall not be used to look into private residential or commercial property. This type of activity would be defined as "Intrusive Surveillance" under RIPA and the City Council is not authorised to carry out this type of surveillance. To minimise the risk of this happening collaterally, "Privacy Zones" may be programmed into the System as required in order to ensure that the cameras cannot survey the interior of any private residential or commercial property within range of the System. These zones may only be altered by the authorised System Manager or Administrator

2.5. Notwithstanding paragraph 2.4, there may be circumstances when it will be necessary to suspend a privacy zone in order to utilise a camera in the detection or prevention of crime. As this will result in Intrusive Surveillance, only the Police or one of the other Public Authorities who are authorised under RIPA, could undertake this activity. The System Manager or Administrator must be satisfied that a proper authorisation for Intrusive Surveillance has been submitted before agreeing to the privacy zones being removed and the System must be returned to its original privacy operation as soon as the particular activity has been concluded. Any subsequent footage should be passed to the Authorised Authority and they will retain responsibility for it.

Monitoring and Recording Facilities

- 2.6. Different methods of transmission operate within each system
- 2.6.1. the 'fixed' system cameras transmit images via a cable infrastructure back to the central Control Room, where they can be viewed and stored in a digital archive for 31 days
 - 2.6.2. the vehicle-based systems, do not transmit images externally but record data within each vehicle, however the images are stored on VHS tape and stored according to the system operating procedure.
 - 2.6.3. the OCTV (GSM) system transmits images over the mobile telephone network back to a dedicated receiving laptop PC with the appropriate modem connection. There is also a dedicated 8-day hard drive digital storage component contained within the camera unit
 - 2.6.4. the WiFi system images are fed into the City Council's internal network and distributed from the central NVRS server around the WCC intranet to approved user PC's at the satellite monitoring stations. The main NVRS server also functions as the archive storage of the recorded images which can be accessed from approved PC's around the network
- 2.7. Secondary monitoring (Satellite Monitoring Stations) of the System will be subject to this Code of Practice together with the systems Standard Operating Procedures (SOP) and any relevant site instruction, which details specific requirements for the remote stations.

Recording Policy

2.8. Assuming all equipment is functioning it is the City Council stated CCTV policy and Data Protection registration that :-

2.8.1. All images from the fixed cameras will be constantly recorded in time-lapse mode (not exceeding 2 frames per second) onto a digital recording system and all images will be kept for a period of 31 days.

2.8.2. Images from the vehicle-based cameras will be recorded on the on-board equipment during each surveillance period in both real-time and time-lapse mode onto 3-hour SVHS videotape or digital recording system and all images will be kept for a period of 31 days.

2.8.3. the OCTV (GSM) units, when deployed and for that duration only, will initially record the images onto the integrated digital storage contained within the camera unit. This can then be downloaded onto the associated portable PC

2.8.4. WiFi images are recorded in 'real-time' on the main NVRS server and are kept for 31 days

2.9. 'Fixed' system images from selected cameras may be recorded in real time, at the discretion of the CCTV operators or as directed by the System Manager, onto dedicated real time recorders. This discretion is only to be exercised where the CCTV operator, as defined by this Code, identifies an incident.

CCTV Signs

2.10. In accordance with the Data Protection Act 1998, signs must be displayed which are clearly visible and legible notifying the general public that continuous CCTV monitoring is taking place in the area, the reason for the monitoring and a contact telephone number.

Covert use of CCTV cameras

2.11. None of the cameras forming part of the public space monitoring System are installed in a covert manner.

2.12. Nevertheless, there may be times when an individual will not be aware that he/she is the subject of filming, for instance where the CCTV Operator is directed by an investigating officer to carry out specific surveillance of an individual's movements. This is a necessary and fundamental feature of any overt CCTV system and in those instances, the provisions of RIPA must be complied with, especially where the footage might be called upon to be used in evidence in any subsequent proceedings.

2.13. In urgent cases, where the System is deployed as an immediate response to a current event, and where the purpose of the deployment is to secure personal data, then RIPA authorisation may be given orally, with a written record being made as soon as practicable thereafter.

2.14. See Section 8 and the RIPA Code for further information.

Recording sound

The System on the whole does not record sound. There is capability for noise-monitoring units to be attached to the WiFi enabled cameras but these can only record noise levels/frequencies. All steps will be taken to ensure that these monitors do not record the spoken word.

Rapidly deployable cameras

2.15. From time to time rapidly deployable cameras may be used as part of this System. These are individual cameras which can be temporarily fixed into specific locations and that can transmit data back to the control room. The use of such cameras, and the data produced by virtue of their use, will always accord with the objectives of the System and in accordance with the Code *except where cameras are deployed for directed covert surveillance? Then under RIPA code – justified interference with human rights.*

2.15.1. OCTV (GSM) cameras are used as rapidly deployed cameras and are not always connected into a permanent system. The images are stored in the camera unit and are downloaded regularly to a laptop computer at the location. Their operation, storage and recording policy will comply with this Code (*although at present the recording policy does not say how long these images will be stored for*).

2.15.2. WiFi units are also designed as rapidly deployable cameras in that their images may be transmitted without the need for specific site cabling to the nearest wireless node and thence into the network.

2.15.3. the vehicles may also be considered rapidly deployable and as such will adhere to the Codes principles.

Operation Orders

2.16. The System Manager will prepare an operational order before any rapidly deployable cameras or the vehicle-based units are deployed. The operational order will:

- clearly define the objectives of the deployment
- outline the results sought
- outline the personnel involved in carrying out the deployment, including identifying the person in charge
- include communications arrangements surrounding the deployment
- set out the handling arrangements of data captured as a result of the deployment
- outline contingency procedures
- confirm that
- where applicable, comply with the RIPA Code and ensure that the relevant authority has been obtained.

3. ACCOUNTABILITY AND PUBLIC INFORMATION

General principle

3.1 Legitimate public concerns exist over the use of CCTV in general and many of the specific guidelines below are designed to satisfy the community that the use of the System is subject to adequate supervision and scrutiny.

Annual Report

3.2 An annual report will be produced. Statistical and other relevant information, including any complaints made, will be included in the report. Copies of the annual report will be made available to anyone requesting it. Additional copies will be lodged at (*name and address of libraries, stations, and One-stop shops*).

Control Room Access

3.3 For reasons of security and confidentiality, access to the CCTV control rooms including the Satellite Monitoring Stations are restricted in accordance with this Code. Access to the Control Centre will only be given to those who need such access for official purposes i.e. to carry out some official function and/or investigation for which they have personal responsibility).

3.4 However, in the interest of openness and accountability, anyone wishing to visit the room may be permitted to do so, subject to the prior written approval of the System Manager. Whilst these visitors are present within the control centre, operators will endeavour to maintain cameras on a long-range view. However, in showing the capabilities of the system or due to operational use it is likely that images containing personal data will be seen on occasions. Therefore, all persons given access to the Control Centre will be required to sign a Declaration of Confidentiality (see para 6.3)

3.5 General visitors to the control room will not be permitted to make requests to view specific stored material or give instruction to members of staff regarding the control of cameras.

3.6 It is the responsibility of the Satellite Site Manager to ensure that only authorised staff view the images and that compliance with the DPA is not compromised.

3.7 It should be noted that the Divisional Police stations within the Borough also have satellite viewing stations and are therefore under Metropolitan Police Control as regards access

Enquiries and Complaints

3.8 Any enquiries or complaints regarding the System (with the exception of the WiFi System) should be made to the Head of Crime and Disorder Reduction and CCTV at: Room 57 Council House, 97 – 113 Marylebone Road NW1 5PT. The post holder will aim to acknowledge complaints in writing within seven days.

3.9 During the WiFi pilot programme, the WiFi System Administrator will be responsible for all enquires and complaints regarding the WiFi System to whom all complaints should be addressed.



3.10 Should the initial response to the complaint be unsatisfactory then complainants will be given the opportunity to take the matter further, in accordance with the City Council's internal complaint procedure. Complaints against individual members of the Metropolitan Police Service will be referred to their complaint procedure. Copies of the complaints booklet are available from Room 57 Council House, 97 – 113 Marylebone Road NW1 5PT.

3.11 The System Manager (and the WiFi System Administrator during the initial pilot) will record all written complaints and report them to the System Owner quarterly. These in turn will be included in the Annual Report.

4. ASSESSMENT OF THE SYSTEM AND CODE OF PRACTICE

Evaluation

4.1 The System will be independently evaluated once every two years to establish whether the purposes of the system are being complied with and whether objectives are being achieved. The evaluation will incorporate such things as (for example, but not limited to):

- An assessment of the impact upon crime
- An assessment of the impact on town centre business
- An assessment of neighbouring areas without CCTV
- The views and opinions of the public
- The operation of the Code of Practice
- Whether the purposes for which the system was established are still relevant
- Cost effectiveness
- Compliance with the Code of Practice

The results of the evaluation will be published and will have a bearing on the future functioning, management and operation of the system.

Monitoring

4.2 The System Operator will accept day-to-day responsibility for the monitoring, operation and evaluation of the System and the implementation of this Code of Practice and Manual.

4.3 The System Manager will carry out regular (daily), checks on the document systems to ensure that the Manual is being put into practice.

Audit

4.4 The System Auditor may call unannounced at any time to carry out an examination of the control room records, history and content of Recorded Material I.

Independent Inspection

4.5 A vetted independent body of individuals (Community Observers) drawn from the local community make regular visits and have a responsibility for inspecting the operation of the system.

4.6 Regular 'spot-check' visits will be made to the Central control room to examine the control room documents to ensure that the CCTV Operator, System Operator, and System Manager are operating in accordance with this Code and the Manual. The Community Observers will be permitted access to the CCTV monitoring room, without prior notice. Their findings will be reported to the Auditor and their visit recorded

4.7 Community Observers will be required to sign a declaration of confidentiality

5. STAFFING & OPERATION OF THE CONTROL ROOM

Primary Control

5.1 Only authorised and trained CCTV Operators, the System Operator, the System Manager or the System Manager's Deputy will carry out monitoring operations on any of the equipment and products located within the CCTV Control Room.

5.2 Only authorised and trained CCTV Operators will carry out monitoring at any satellite monitoring station

Security Vetting

5.3. Before commencing , monitoring personnel will be subjected to full security screening up to and including Metropolitan Police CTC level.

5.4. The System Manager or their departmental deputy is responsible for vetting all monitoring staff in line with the British Security Industry Association Standard 7858 and/or any other Security Procedure.

Control and operation of cameras

5.1 Any person operating the cameras will act with integrity at all times.

5.2 Every use of the cameras will accord with the purposes and key objectives of the System and shall be in compliance with this Code of Practice.

5.3 Directed surveillance or surveillance which may otherwise be considered to be covert will only be performed in accordance with the RIPA Code.

5.4 Monitoring personnel are not permitted to change system settings set by the System Manager or interfere with the equipment in any way other than that required for day to day control and operation of the System whether requested to by other Westminster personnel or not.

5.5 Personnel should also comply with their specific individual requirements of their site instructions or SOP

Training

5.6 CCTV Operators will be fully trained in the use of each item of equipment;

5.7 Each operator will be personally issued with a copy of this Code, the appropriate SOP, any relevant site instruction and the RIPA Code and will be given training to ensure compliance with each as far as is reasonably practicable at all times.

5.8 The System Operator and each dedicated CCTV Operator will be required to undertake the SITO CCTV Control Room Operator's Course and be given training in all relevant social and legal issues.

5.9 CCTV Operators will undertake continuation training on a regular basis.

Declaration of Confidentiality

5.10 Every individual with any responsibility under the terms of this Code and who has any involvement with the CCTV System to which they refer, will be required to sign a declaration of confidentiality (see para 6.3).

Discipline

5.11 Each CCTV Operator will be subject to the disciplinary code of their appropriate employer. Any breach by a CCTV Operator of the **Code of Practice** or **SOP**, or of any aspect of confidentiality contained therein, will be dealt with in accordance with the appropriate discipline regulations.

5.12 The System Manager will accept primary responsibility for ensuring there is no breach of security and CCTV Operators comply with the Code of Practice and Manual. The (System Operator) has day-to-day responsibility for the management of the room and for enforcing the discipline rules.

5.13 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.

Operation of the System by the Police or other approved agencies

5.14 Under extreme circumstances e.g. a major public order incident, the Police may make a request to take control of part of the System to which this Code of Practice applies.

5.15 Only requests made on the written authority 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 most senior representative of the System Owners (or designated deputy of equal standing).

5.16 In the event of such a request being permitted, the Control Room will continue to be staffed, and equipment operated by those personnel who are authorised to do so and who fall within the terms of this section.

5.17 It will also be permissible for police or other authorised agencies to operate, after relevant training, monitoring stations within the overall operation without affecting the continued operation of the rest of the system.

5.18 In very extreme circumstances e.g. terrorist action, a request may be made for the Police to take total 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. A request for total exclusive control must be made in writing by a police officer not below the rank of Deputy Assistant Commissioner (*or person of equal standing*) to the most senior officer of the System Owner (or designated deputy of equal standing).

5.19 Joint operations in the Control Room involving the Police or other approved Government agencies may take place with the proper approval from the System Owner but all personnel involved in the joint operation shall be bound by the terms of this Code.

6. CONTROL ROOM SECURITY

Visits to the Control Room or Satellite Monitoring Stations

6.1 Entry to the CCTV control room is not allowed, except for authorised officers, without proper and sufficient reasons as previously stated in section 3.3 to 3.6 of this Code.

6.2 To ensure security and confidentiality, visits to the CCTV control rooms are restricted and will only be allowed with the approval of the System Manager and with prior written notice. Such visits will be made under the supervision of the CCTV Operator and will be recorded in the Visitor Book kept in the CCTV control room.

Declaration of Confidentiality

6.3 All visitors to the CCTV control room will be required to sign a Declaration of Confidentiality which states:

“Access to the CCTV control room may mean that you are exposed to personal data that is being processed or being held within the centre. You are therefore required to sign as a condition of entry to confirm that you understand the obligations placed upon you in relation to that confidential information:

I understand that in accordance with the Data Protection Act 1998, any personal data that comes to my attention while in the CCTV control room is protected from disclosure by the principles of the Act, that all persons captured on CCTV have a right to privacy by virtue of Article 8 of Schedule 1 to the Human Rights Act 1998 and I undertake to respect that persons right to privacy.

I, therefore, agree not to disclose any personal details that may come to my attention to anyone outside of the CCTV Control Room.”

6.4 A restricted access notice must be positioned next to the door of all Control Rooms, including satellite monitoring stations advising visitors that access to the control room is restricted and that viewing of the monitors may be denied.

Security

6.5 Authorised personnel will be present at all times when the equipment is in use.

6.6 If the control room or associated equipment is to be left unattended for any reason it will be securely locked.

6.7 The System Manager is responsible for ensuring access to the control room is in accordance with this Code and.

7. HANDLING OF RECORDED MATERIAL

Guiding Principles

7.1 All information recorded by the System has the potential of being material that has to be admitted in evidence, especially as the key objective of the System is the detection and prevention of crime.

7.2 It is critical therefore that all residents, businesses and visitors to the area of CCTV coverage must have total confidence that any information that may be recorded while they go about their every day activities, is handled with due regard to their individual right to respect for their private and family life, as well as in accordance with the following guidelines:

- i) All information should be treated strictly in accordance with this Code and the Manual, from the moment it is delivered to the control room until its final destruction;
- ii) The audit trail of Recorded Material will ensure that a particular image can be identified at any time;
- iii) Access to, and the use of, Recorded Material will be strictly for the purposes defined in this Code of Practice only;
- iv) Under no circumstances, whether supported by a signed authority from a Council Officer, Policeman or other purported authority shall recorded material be copied, sold, otherwise released or used for commercial purposes or for the provision of entertainment.
- v) The showing of Recorded Material to members of the public will take place only in accordance with this Code and the law.

Data Retention

7.3 Recorded Material will be stored securely and retained for a period of 31 days before being destroyed and overwritten.

7.4 Where video recording (analogue) is used these will be magnetically erased (de-gaussed) after 31 days and each tape will only be used a maximum of 12 times, after which it will be erased and destroyed.

7.5 Where digital recording is used, an 'overwrite' facility will be used to ensure out of date data is not retained unnecessarily after 31 days.

7.6 Where court proceedings are instigated and the CCTV footage becomes evidence, the data will be extracted from the System, clearly labelled and made tamper-proof and will be kept securely in a locked safe until required at court. The release of data will be carried out under the direction and supervision of the System Manager.

7.7 The CCTV Operator who recorded the evidence may be required to produce a witness statement. In some instances, the Operator may also be required to attend court and give oral evidence, although any such evidence should be limited to confirmation that the equipment was used and the data recorded by the Operator.

7.8 Both evidential and working copies of images may be supplied to the Police or other enforcement agencies, which have a statutory authority to investigate and/or prosecute offences, within the systems objectives as set out in para 1.4. Neither evidential nor working copies of images will be released without the authority of the Systems Manager and in accordance with paragraph 8.3.

Release of data to a third party

7.9 Every request for the release of personal data generated by this System will be channelled through the System Manager. The System Manager will ensure the principles to this Code, and specifically the Data Protection Principles, are followed at all times.

7.10 Where there is a risk that data passed to a third party may contain personal data of an individual from whom consent to disclose such data has not been obtained; and where release of such data is not exempted from the Data Protection Principles, then the Data Controller must ensure that no such individual can be identified from the released data. This should be achieved by using appropriate editing techniques so that such individuals cannot be identified on the recording (i.e. pixelation).

7.11 Members of the Police service or other enforcement agencies who have been designated to investigate incidents or have a statutory authority to investigate and/or prosecute offences may, subject to compliance with this Code, release details of recorded information to the media, only in an effort to identify alleged offenders or potential witnesses. This will only be with the joint agreement of the investigating police officer and the System Manager and for which a licence will be issued.

7.12 It may be beneficial to make use of Recorded Material for the training and education of those involved in the operation and management of CCTV Systems, and for those involved in the investigation, prevention and detection of crime. Any such use of Recorded Material will only be used for bona fide training and education purposes.

8. DATA PROTECTION, HUMAN RIGHTS AND PRIVACY

Data Protection

8.1 The Information Commissioner has been notified of the existence of the System in accordance with the Data Protection Act 1998.

8.2 All personal data will be processed in accordance with the principles of the Data Protection Act, as follows:

- i) personal data shall be processed fairly and lawfully;
- ii) personal data shall be obtained only for specific and lawful purposes and shall not be further processed in any manner incompatible with that purpose;
- iii) Personal data will only be held which is adequate, relevant and not excessive in relation to the purpose for which the data is held;
- iv) steps will be taken to ensure that personal data is accurate and, where necessary, kept up to date;
- v) personal data that is retained for any purpose shall be held for no longer than is necessary for the purpose ;
- vi) individuals will be allowed access to information held about them and, where appropriate, permitted to correct or erase it, in accordance with the Data Subjects' Access rights (see Section 10);
- vii) Appropriately technical and secure organisational measures will be put in place to prevent unauthorised or unlawful processing of personal data and accidental loss or destruction of, or damage to, personal data.

8.3 The Data Controller is under a duty to comply with these principles and remains responsible for the actions of any third party Data Processor. Therefore, the Data Controller will ensure that processing carried out by a third party Data Processor will only be by written contract, which obliges the Data Processor to comply with the Seventh Data Protection Principle (see 8.2vii above)

8.4 Further information on compliance with the Date Protection Act and the handling of Subject Access Requests can be found on the City Councils Website (The Wire)

Human Rights

8.5 The European Convention of Human Rights has now been incorporated into UK law by the Human Rights Act 1998. One of the fundamental rights is that everyone has the right to respect for private and family life, home and correspondence.

8.6 However, this is not an absolute right, which means that a public authority can interfere with this right, provided such interference is in accordance with the specified grounds. One of these grounds is the

prevention of disorder or crime, but the interference must be proportionate to that aim.

8.7 By its very nature, the use of a CCTV System will result in the surveillance of individuals, and is likely to record private information, but this can be a justified interference of the right to privacy on the grounds of its predominant purpose, namely the prevention of crime and disorder.

8.8 Nevertheless, the System will be operated in a way that will respect an individual's right to privacy and any interference with that right will be in accordance with the statutory guidelines and will be proportionate to the objectives of the System.

Freedom of Information Act 2000

8.9 All records retained by the CCTV control room are subject to this Act. Further information about compliance with FoI and the handling of information requests can be found on the City Council Website (The Wire)

Regulation of Investigatory Powers Act 2000 (RIPA)

8.10 RIPA provides guidelines for safeguarding an individual's right to privacy where a public authority undertakes covert surveillance.

8.11 It is generally accepted that provided the CCTV System is used in line with the defined objectives (see 1.5), then the use would be described as overt surveillance and as such the provisions of the Act will not apply.

8.12 However, the System is capable of being deployed for directed covert surveillance, where there is a possibility that an individual will be filmed for the purpose of a specific investigation or operation and private information about that individual will be obtained. In these circumstances, the Act will apply.

8.13 For the avoidance of doubt, in all cases where the System is being deployed for a specific purpose and where specific individuals are going to be filmed the CCTV Operator must be in possession of an official RIPA authorisation from the relevant agency. A copy of the authorisation must be retained for the records of the Control Room and brought to the attention of the Control Room manager. Please refer to the RIPA Code of Practice for further information.

9. DATA SUBJECT ACCESS REQUESTS

Applying to view Recorded Material

9.1 An individual, who believes that his personal data has been recorded by the System, may make a request to the Data Controller to have access to that data, either by requesting a copy of the Recorded Material containing his personal data or by requesting a viewing.

9.2 The individual must provide adequate details such as the date, time, location and a brief description of the incident. The recording equipment can produce date/time indexing on recorded information.

9.3 An example of the Data Subject Access Request Form is attached to this Code and there is an administration charge of £10 for each request.

9.4 Requests to view Recorded Material after 31 days of the incident cannot be processed as the material would have been erased in accordance with the 31-day rotation system.

9.5 Once a request has been made to the Data Controller, the Systems Manager will be instructed to immediately set aside the relevant Recorded Material from the 31-day rotation system and label it accordingly.

9.6 The Data Controller has 40 days within which to comply with a request for access/viewing, during which time he will determine whether the individual making the request is the Data Subject. Accordingly, an individual will be asked to produce proof of identity, such as a passport, driver's licence or similar document with an up-to-date photograph. If a vehicle is involved in the request, the individual making the request will be asked to provide the vehicle registration document.

Exemptions to the Provision of Information

9.7 Data Subject Access Requests can be refused if the personal data was processed for:

- i) the prevention or detection of crime
- ii) the apprehension or prosecution of offenders
- iii) the assessment or collection of any tax or duty

Disproportionate Effort

9.8 The Data Controller cannot disclose third party data without the consent of the third party and the Data Controller must ensure that no individual other than the Data Subject can be identified from the data. Where this is not possible or practicable, and/or to process the data requires more effort than is reasonable in the circumstances, then a request for access may be refused.

9.9 The Data Controller can also refuse a request for access if searching for the correct data would require disproportionate effort, for instance, where insufficient or inaccurate information has been provided by the Data Subject in their request.

9.10 In applying these exemptions, consideration must be given to whether non-disclosure would be likely to prejudice the data subject in any way.

Each and every request for access will be assessed on its own merits and general 'blanket exemptions' should not be applied.

Request accepted

9.11 If the request is accepted the System Manager will arrange a convenient time and date for viewing to take place that will be supervised by the Systems Manager.

9.12 Where cameras have been recorded in "time-lapse" mode, there may be small gaps in the filming and the incident, which the individual has requested to see, may not be filmed in full.

9.13 Where an individual may wish to produce the data recorded by the System as evidence in any court proceedings, a witness summons or court order will be required to release the Recorded Material.

9.14 Where criminal proceedings involving the data subject have been instigated then the relevant enforcement agency (e.g. WCC, police, Customs) , will assume the responsibility of any recorded evidence removed from the Control Room. This will be disclosed to the defendant (data subject) by the relevant prosecuting authority in accordance with the rules of disclosure of evidence.

10. CCTV COPY PRINTS

Guiding Principles

10.1 A copy print is a **copy** of an image or images which already exist on videotape / computer disc. Copy 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 SOP.

10.2 Copy Prints can be made in a number of formats; video (VHS) prints, DVDs, CDs, mini DV tapes and still images

10.3 Copy prints contain data and will therefore only be released under the terms paragraph 8.3 of to this Code ('Release of data to third parties').

10.4 If prints are released to the media, in an effort to identify alleged offenders or potential witnesses, full details will be recorded in accordance with the SOP.

10.5 A record will be maintained of all copy print productions in accordance with the SOP.