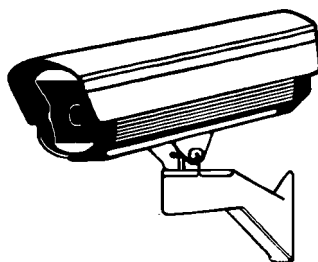


LONDON BOROUGH OF HAMMERSMITH AND FULHAM

in partnership with

The Metropolitan Police

**Code of Practice
for the operation of
Public Space Closed Circuit Television**



Contents

Index	Page 1
Acknowledgement	Page 2
Certificate of Agreement	Page 3
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 system and the code of Practice	Section 5
Human Resources	Section 6
Control and Operation of the cameras	Section 7
Access to, and Security of, Monitoring Room and/or Associated Equipment	Section 8
Management of Recorded Material	Section 9
Video Prints	Section 10
Appendices	
Key Personnel and their Responsibilities	Appendix A
Extracts from the Data Protection Act, 1998	Appendix B
National Standard for the Release of Data to Third Parties	Appendix C
Restricted Access Notice	Appendix D
Declaration of Confidentiality (Operator/Manager)	Appendix E
Integrated Systems. Agreement	Appendix F
Subject Access Request Form	Appendix G
Camera Locations	Appendix H
Regulation of Investigatory Powers Act Guiding Principles	Appendix I

This Code of Practice applies primarily to the Public Space CCTV system operated and owned by the Hammersmith & Fulham Council. It also applies to certain other CCTV cameras owned by LBHF such as “standalone” mobiles and the Small Retailers CCTV systems.

Other Council departments who operate CCTV cameras for their own purposes must have their own Code of Practice which must reflect the principles contained in this document.

Complaints:

Any complaint regarding the operation of the Hammersmith & Fulham Council CCTV System should be addressed to:-

The Emergency Planning & Risk Manager

London Borough of Hammersmith & Fulham

Room 313

Hammersmith Town Hall

King Street

London

W6 9JU

Acknowledgement

Our Code of Practice is the copyright of the London Borough of Hammersmith & Fulham. It is based upon a Model Code of Practice prepared by:

The Standards Committee of the CCTV User Group

PO Box 6023

Leighton Buzzard

Bedfordshire

LU7 0YU

The Model Code of Practice is the copyright of the CCTV User Group and subject to their conditions.

**Code of Practice in Respect of the
Operation of
CCTV in Hammersmith & Fulham Borough**

***Agreed by
London Borough of Hammersmith & Fulham
And The Metropolitan Police***

Certificate of Agreement

The content of both this Code of Practice and the Operational Procedures Manual are hereby approved in respect of the London Borough of Hammersmith & Fulham Closed Circuit Television System and will be complied with by all who are involved in the management and operation of the System.

Signed for and on behalf of London Borough of Hammersmith & Fulham

Signature: Geoff Alltimes.....

Name: Geoff Alltimes

Position held: Chief Executive & Chair of the CDRP

Dated the26th..... day ofJuly..... 2005

Signed for and on behalf of Metropolitan Police- Hammersmith & Fulham BOCU

Signature: Heather Valentine.....

Name: Heather Valentine

Position held: Borough Commander

Dated the26th..... day ofJuly..... 2005

Section 1 Introduction and Objectives

1.1 Introduction

A Closed Circuit Television (CCTV) system has been introduced to some public areas within the London Borough of Hammersmith & Fulham (LBHF). This system, known as the 'The Integrated Public Safety System', comprises a number of cameras installed at strategic locations. Most of the cameras are fully operational with pan, tilt and zoom facilities. Others are fixed cameras, images from all are presented in a purpose built control room. Secondary monitoring and control facilities are located at Hammersmith and Fulham Police Control rooms and certain other approved locations, but there are normally no recording facilities at any location other than the CCTV monitoring room.

The Integrated Public Safety CCTV System exists from the formation of a partnership between LBHF and the Metropolitan Police (Hammersmith & Fulham BOCU) who have both certified on the previous page their acceptance of the requirements of this code. Additionally we will seek to integrate our system with new partners whose CCTV systems will be data protection compliant.

We will seek to integrate our system with new partners whose CCTV systems will be data protection compliant.

For the purposes of this document, the 'owner' of the system is the London Borough of Hammersmith & Fulham. The Emergency Planning and Risk Manager will act for the Owners.

For the purposes of the Data Protection Act the 'data controller' is the London Borough of Hammersmith & Fulham. The Council's "Information Manager" –formerly the Data Protection Officer will act in this capacity

The 'system manager' is the CCTV Development & Security Adviser.

Details of The Integrated Public Safety CCTV system has been registered with the Information Commissioner.

Details of key personnel, their responsibilities and contact points are shown at Appendix A to this Code.

1.2 Partnership statement in respect of The Human Rights Act 1998

- 1.2.1 The partnership recognises that public authorities and those organisations carrying out functions of a public service nature, are required to observe the obligations imposed by the Human Rights Act 1998, and consider that the use of CCTV in the Hammersmith & Fulham area is a necessary, proportionate and suitable tool to help reduce crime, reduce the fear of crime and improve public safety.
- 1.2.2 Section 163 of the Criminal Justice and Public Order Act 1994 creates the power for local authorities to provide closed circuit television coverage of any land within their area for the purposes of crime prevention or victim welfare and it is also considered a necessary initiative by the Partners towards their duty under the Crime and Disorder Act 1998.
- 1.2.3 It is recognised that operation of the Integrated Public Safety CCTV System may be considered to infringe on the privacy of individuals. The Partnership recognise that it is their responsibility to ensure that the scheme should always comply with all relevant legislation, to ensure its legality and legitimacy. The scheme will only be used as a proportional response to identified problems and be used only in so far as it is necessary in a democratic society, in the interests of national security, public safety, the economic well being of the area, for the prevention and detection of crime or disorder, for the protection of health and morals, or for the protection of the rights and freedoms of others.
- 1.2.4 The Codes of Practice and observance of the Operational Procedures contained in the manual shall ensure that evidence is secured, retained and made available as required to ensure there is absolute respect for everyone's right to a free trial. Any images received from a system integrated into the councils CCTV system, will be treated with all due regard to this Code of Practice.(See Appendix F)

1.2.5 The Integrated Public Safety CCTV System shall be operated with respect for all individuals, recognising the right to be free from inhuman or degrading treatment and avoiding discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

1.3 Objectives of the System

1.3.1 The objectives of the Integrated Public Safety CCTV System as determined by the London Borough of Hammersmith & Fulham and The Metropolitan Police which form the lawful basis for the processing of data include:-

- *To assist in the prevention of crime and anti social behaviour*
- *To assist in the detection of crime and other offences*
- *To assist in the identification, apprehension and prosecution of offenders*
- *To reduce public fear of crime (which includes LBHF residential estates)*
- *To assist in Traffic Management & Traffic Enforcement*
- *To assist with Town Centre Management*
- *To assist in the management of emergency services' response to major incidents*
- *Effective and efficient operation of council policies and procedures*

1.3.2 Within this broad outline, Heather Valentine- Police Borough Commander, in partnership with Geoff Alltimes- Chief Executive of London Borough of Hammersmith & Fulham and Chair of the Crime & Disorder reduction Partnership, has drawn up, and published specific key objectives (which will be reviewed annually) based on local concerns.

1.4 Procedural Manual

This Code of Practice (hereafter referred to as 'the Code') is supplemented by a separate 'Operational Procedures Manual' which offers instructions on all aspects of the day to day operation of the system. To ensure the purpose and principles (see Section 2) of the CCTV system are realised, the procedures manual is based and expands upon the contents of this Code of Practice.

Section 2 Statement of Purpose and Principles

2.1 Purpose

The purpose of this document is to state the intention of the owners and the managers, on behalf of the Partnership as a whole and as far as is reasonably practicable, to support the objectives of the Integrated Public Safety System, (hereafter referred to as 'The System') and to outline how it is intended to do so.

2.1.1 The 'Purpose' of the system, and the process adopted in determining the 'Reasons' for implementing 'The System' are as previously defined in order to achieve the objectives detailed within Section 1.

2.2 General Principles of Operation

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

2.2.2 The operation of the system will also recognise the need for formal authorisation of any 'Directed' surveillance as required by the Regulation of Investigatory Powers Act 2000 and the Metropolitan Police Service policy.

2.2.3 The system will be operated in accordance with the Data Protection Act at all times.

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

2.2.5 The system will be operated with due regard to the principle that everyone has the right to respect for his or her private and family life and their home.

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

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

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

2.3 Copyright

Copyright and ownership of all material recorded by virtue of the System or produced in respect of its operation will remain with the LBHF.

2.4 Cameras and Area Coverage

2.4.1 The areas covered by CCTV to which this Code of Practice primarily refers, are those public areas within the responsibility of the operating partners within the Borough of Hammersmith & Fulham. These are generally the main town centre areas and transport interchange areas and will change as the system expands.

- 2.4.2 From time to time mobile cameras may be temporarily sited within the area. The use of such cameras, and the data produced by virtue of their use, will always accord with the objectives of the CCTV System and be governed by these Codes and Procedures. The use of mobile cameras will be subject to authorisation by both the Police Borough Commander (or Deputy), and the Council's Emergency Planning and Risk Manager. Any such use will be subject of notification to the Council's Assistant Director responsible for the Safer Communities Division, the Leader, Opposition Leader and the Deputy for Social Inclusion.
- 2.4.3 Some of the cameras offer full colour, pan tilt and zoom (PTZ) capability, some of which may automatically switch to monochrome in low light conditions.
- 2.4.4 None of the cameras forming part of the System will be installed in a covert manner. Some cameras may be enclosed within 'All weather domes' for aesthetic or operational reasons but the presence of all cameras will be identified by appropriate signs displayed in the area.

2.5 Monitoring and Recording Facilities

- 2.5.1 A secure monitoring control room is provided which will be staffed 24 hours a day. The CCTV equipment has the capability of recording all camera images simultaneously throughout every 24-hour period. Separate arrangements exist in respect of traffic enforcement cameras and this activity is governed by the Council's Code of Practice for the Operation of CCTV Enforcement Cameras. Images from Transport for London (TfL) cameras available in the control room may be recorded when necessary.
- 2.5.2 Secondary monitoring equipment may be located in police premises, approved football stadia control rooms or the Council's own incident control room. No equipment, other than that housed within the main CCTV control room will normally be used to, or be capable of recording images from any of the cameras. "Monitoring only" facilities may be authorised by the Emergency Planning Manager if required. Links are available to Metropolitan Police call control centres.
- 2.5.3 CCTV operators are able to record images from selected cameras in real-time, produce hard copies of recorded images, replay or copy any pre-recorded data at their discretion and in accordance with the Code of Practice. All viewing and recording equipment shall only be operated by trained and authorised users.

2.6 Human Resources

- 2.6.1 Unauthorised persons will not have access to the control room without an authorised member of staff being present.
- 2.6.2 The monitoring room shall be staffed by specially selected and trained operators in accordance with the strategy contained within the procedural manual.
- 2.6.3 All operators shall receive training relevant to their role in the requirements of the Human Rights Act 1998, Data Protection Act 1998, Regulation of Investigatory Powers Act 2000 and the Codes of Practice and Procedures. Further training will be provided as necessary.

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 of Practice and the Procedures Manual.

2.8 Operators Instructions

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

2.9 Changes to the Code or the Procedural Manual

- 2.9.1 Any major changes to either the Code of Practice or the Procedural Manual, (i.e. such as will have a *significant* impact upon the Code of Practice or upon the operation of the system) will take place only after consultation with, and upon the agreement of all signatories to these Codes.
- 2.9.2 A minor change, (i.e. such as may be required for clarification and will not have such a significant impact) may be agreed between the manager and the owners of the system.

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 the 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.

3.2.2 The 'data controller' for the System is the *London Borough of Hammersmith & Fulham* and day to day responsibility for the data is currently devolved to the Safer Communities Division Security Manager and his/her deputy.

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

- i) All personal data will be obtained and processed fairly and lawfully.
- ii) Personal data will be held only for the purposes specified.
- iii) Personal data will be used only for the purposes, and disclosed only to the people, shown within these codes of practice.
- iv) Only personal data will be held which is adequate, relevant and not excessive in relation to the purpose for which the data is held.
- v) Steps will be taken to ensure that personal data is accurate and where necessary, kept up to date.
- vi) Personal data will be held for no longer than is necessary.
- vii) Individuals will be allowed access to information held about them and, where appropriate, permitted to correct or erase it.

- viii) Procedures will be implemented to put in place security measures to prevent unauthorised or accidental access to, alteration, disclosure, or loss and destruction of, information.

3.3 Request 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 system manager or Information Manager.
- 3.3.2 The principles of Sections 7 and 8, 10 and 12 of the Data Protection Act 1998 (Rights of Data Subjects and Others) shall be followed in respect of every request. Sections 7 & 8 are reproduced as Appendix B to these codes.
- 3.3.3 If the request cannot be complied with without identifying another individual, permission from all parties must be considered (in the context of the degree of privacy they could reasonably anticipate from being in that location at that time) in accordance with the requirements of the legislation.
- 3.3.4 Any person making a request must be able to satisfactorily prove their identity and provide sufficient information to enable the data to be located. The appropriate 'Subject Access' request forms are included at Appendix G.

3.3.5 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:

- 3.3.6 Personal data processed for any of the following purposes -

- i) the prevention or detection of crime
- ii) the apprehension or prosecution of offenders

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

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

3.4 Criminal Procedures and Investigations Act, 1996

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

Section 4 Accountability and Public Information

4.1 The Public

- 4.1.1 For reasons of security and confidentiality, access to the CCTV monitoring room is restricted and controlled by the Emergency Planning & Risk Manager or his nominee in accordance with this Code of Practice
- 4.1.2 Cameras will not be used to look into private residential property. Where the equipment permits it 'Privacy zones' may be programmed into the system as required in order to ensure that the interior of any private residential property within range of the system is not surveyed by the cameras. If such 'zones' cannot be programmed the operators will be specifically trained in privacy issues.
- 4.1.3 A member of the public wishing to register a complaint with regard to any aspect of the System may do so by contacting the System Manager's office. All complaints shall be dealt with in accordance with London Borough of Hammersmith & Fulham complaints procedure, a copy of which may be obtained from LBHF Emergency Services, Room 313, Hammersmith Town Hall, King Street, Hammersmith, London, W6 9JU. Any staff performance issues identified will be considered under the organisations disciplinary procedures to which all members of London Borough of Hammersmith & Fulham, including CCTV personnel are subject.
- 4.1.4 All CCTV staff are contractually subject to regulations governing confidentiality and discipline. An individual who suffers damage or distress by reason of any contravention of this Code of Practice may be entitled to compensation.

4.2 System Owner

- 4.2.1 The Emergency Planning and Risk Manager, named at Appendix A, being the nominated representative of the system owners, will have unrestricted personal access to the CCTV monitoring room and will be responsible for receiving regular and frequent reports from the manager of the system.
- 4.2.2 London Borough of Hammersmith & Fulham will nominate a committee with a specific responsibility for receiving and considering those reports.
- 4.2.3 Formal consultation will take place between the owners and the managers of the system with regard to all aspects, including this Code of Practice and the Procedural Manual.

4.3 System Manager

- 4.3.1 The nominated manager named at Appendix A will have day-to-day responsibility for the system as a whole.
- 4.3.2 The system manager will ensure that every complaint is acknowledged in writing within five working days which will include advice to the complainant of the enquiry procedure to be undertaken. A formal report will be forwarded to the nominee of the system owner named at Appendix A, giving details of all complaints and the outcome of relevant enquiries.
- 4.3.3 Statistical and other relevant information, including any complaints made, will be included in the Annual Reports of London Borough of Hammersmith & Fulham, which are made publicly available.

4.4 Public Information

4.4.1 Code of Practice

A copy of this Code of Practice shall be published on the council's website at www.lbhf.gov.uk, and copies are available from public libraries. Additionally the codes will be available to the public on request by writing to: London Borough of Hammersmith & Fulham (Emergency Services), Room 313, Hammersmith Town Hall, King Street, Hammersmith, London, W6 9JU

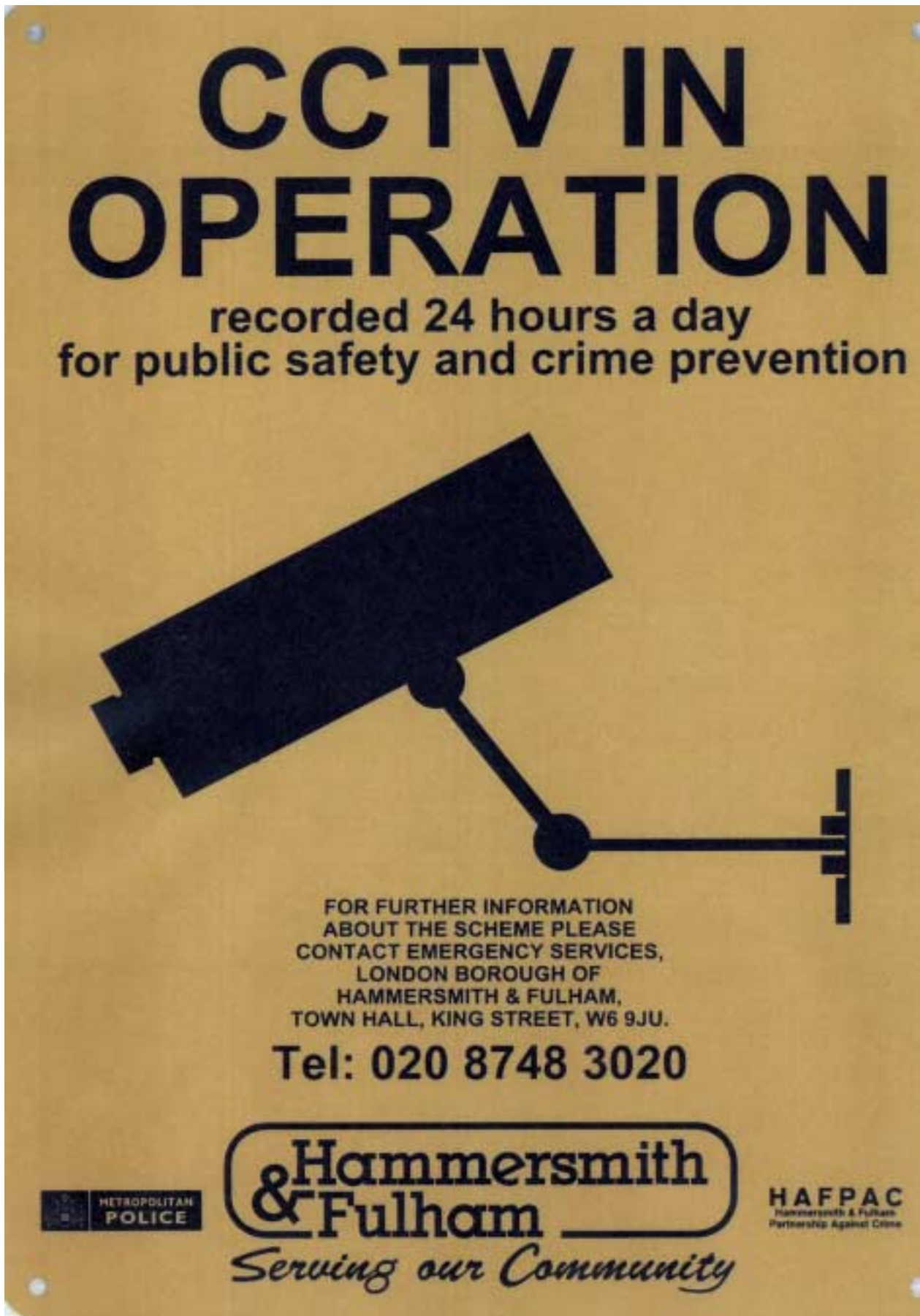
4.4.2 Signs

Signs (as shown below) will be placed in the areas covered by cameras. The signs will indicate:

- i) The presence of CCTV monitoring;
- ii) The 'ownership' of the system;

CCTV Code of Practice for the London Borough of Hammersmith & Fulham

- iii) Contact telephone number of the 'data controller' of the system.



Example of Street sign in use.

Section 5 Assessment of the System and Code of Practice

5.1 Evaluation

5.1.1 Periodically, the System will be independently evaluated to establish whether the purposes of the system are being complied with and whether objectives are being achieved. The evaluation will include:-

- i. An assessment of the impact upon crime*
- ii. An assessment of the incidents monitored by the system*
- iii. An assessment of the impact on town centre business*
- iv. An assessment of neighbouring areas without CCTV*
- v. The views and opinions of the public*
- vi. The operation of the Code of Practice*
- vii. Whether the purposes for which the system was established are still relevant*
- viii. Cost effectiveness*

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

5.1.3 It is intended that evaluations should take place at least every two years.

5.2 Monitoring

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

5.2.2 The system manager shall also be responsible for maintaining full management information as to the incidents dealt with by the monitoring room, for use in the management of the system and in future evaluations

5.3 Audit

5.3.1 The Assistant Director – Safer Communities Division, or a nominee, who is not the system manager will be responsible for regularly auditing the operation of the system and the compliance with this Code of Practice. Audits, which may be in the form of irregular spot checks, will include examination of Control room records, equipment checks and the content of recorded material. As the person to conduct spot checks will need to enter the control room, perhaps while police operations are in progress, consideration must be given as to their suitability and formal approval.

Section 6

Human Resources

6.1 Staffing of the Control Room and those responsible for the operation of the system

- 6.1.1 The CCTV Monitoring Room will be staffed in accordance with the procedures manual. Equipment associated with the System will only be operated by authorised personnel who will have been properly trained in its use and all monitoring room procedures.
- 6.1.2 Every person involved in the management and operation of the system will be personally issued with a copy of both the Code of Practice and the Procedural Manual, and will be required to sign a confirmation that they fully understand the obligations adherence to these documents places upon them and that any breach may be considered as a disciplinary offence. They will be fully conversant with the contents of both documents, which may be updated from time to time, and which he / she will be expected to comply with as far as is reasonably practicable at all times. Additionally they will be required to sign the confidentiality agreement as shown at Appendix E.
- 6.1.3 Arrangement may be made for a police liaison officer to be present in the monitoring room at certain times, or indeed at all times, subject to locally agreed protocols. Any such person must also be conversant with this Code of Practice and associated Procedural Manual.
- 6.1.4 All personnel involved with the system shall receive training from time to time in respect of all legislation appropriate to their role.

6.2 *Discipline*

- 6.2.1 Every individual with any responsibility under the terms of this Code of Practice and who has any involvement with the System to which they refer, will be subject to the LBHF discipline code. Any breach of this Code of Practice or other security breach including any aspect of confidentiality, may be dealt with in accordance with those discipline rules and if appropriate by the instigation of criminal proceedings.
- 6.2.2 Any breach of the Code of Practice by LBHF CCTV operating staff will initially be investigated by the LBHF security manager and / or deputy who will report to the Emergency Planning & Risk Manager and/or System manager.
- 6.2.3 Any breach of the Code of Practice by any police staff will be referred to the Borough Police Commander for appropriate action under Metropolitan Police Service procedures.
- 6.2.4 The System manager will accept primary responsibility for ensuring there is no breach of security and that the Code of Practice is complied with. He/she has day to day responsibility for the management of the room and ensuring that investigations are conducted when necessary and ensuring the discipline rules are enforced. Non-compliance with this Code of Practice 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 of Practice and who has any involvement with the System to which they refer, will be required to sign a declaration of confidentiality. (See example at Appendix E, see also Section 8 concerning access to the monitoring room by others).

Section 7 Control and Operation of Cameras

7.1 Guiding Principles

- 7.1.1 Any person operating the cameras will act with utmost probity at all times and their actions must be justifiable
- 7.1.2 The cameras, control equipment, recording and reviewing equipment shall at all times only be operated by persons who have been trained in their use and the legislative implications of their use.
- 7.1.2 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.
- 7.1.3 Cameras will not be used to look into private residential property. 'Privacy zones' may be programmed into the system (whenever practically possible) in order to ensure that the interior of any private residential property within range of the system is not surveyed by the cameras.
- 7.1.4 Camera operators will 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, group of individuals or property at any time by virtue of the audit of the system or by the system manager.

7.2 Primary Control

- 7.2.1 Only those trained and authorised members of LBHF 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

- 7.3.1 Secondary monitoring facilities are provided at police control rooms at Hammersmith & Fulham, approved football club stadia, the council's own incident control room and Metropolitan Police call control centres.
- 7.3.2 Subject to permission being granted by the primary control room operator, secondary control rooms may take control of the operation of the cameras. The use of secondary control and monitoring facilities will be administered and recorded in full accordance with this Code of Practice and the Procedures Manual and does not diminish in any way the obligations imposed on any of the persons involved to comply with all current legislative requirements.

7.4 Operation of the System by the Police

- 7.4.1 Under extreme circumstances the Police may make a request to assume a degree of overall control of the System to which this Code of Practice applies. 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.
- 7.4.2 In the event of such a request being permitted, the Monitoring Room will continue to be staffed, and equipment operated by, only those personnel who are authorised to do so, and who fall within the terms of Sections 6 and 7 of this Code, who will then operate under the direction of the police officer designated in the written authority.

7.5 Police Liaison

- 7.5.1 All police contact with the CCTV room will be recorded in the control room incident log.
- 7.5.2 The Divisional Crime Prevention Officer/Crime Prevention Design Adviser and the Partnership Inspector are the divisional officers responsible for operational CCTV liaison with the Local Authority.
- 7.5.3 Telephone hotlines and SafetyNet radios are provided in the CCTV control room and police CAD rooms and will link both. Where Police radio or data systems are installed in the CCTV room they must only be monitored by authorised staff and be switched off when non-authorised persons are in the room. The police CAD rooms MUST be informed when this occurs. Whilst it is not expected that CCTV operators will have to transmit on the police radio, there may be very exceptional circumstances when this may be necessary. No person will transmit on any police radio unless they have been trained in the use of the radio and the R/T procedure to be used by a member of police staff. A protocol for the provision of police radio systems will exist.

7.6 Maintenance of the system

- 7.6.1 To ensure compliance with the Information Commissioners Code of Practice and that images recorded continue to be of appropriate evidential quality, the CCTV System shall be maintained in accordance with the requirements of the Procedures Manual under a maintenance agreement.
- 7.6.2 The maintenance agreement will make provision for regular/ periodic service checks on the equipment which will include cleaning of any all weather domes or housings, checks on the functioning of the equipment, and any minor adjustments that need to be made to the equipment settings to maintain picture quality.
- 7.6.3 The maintenance will also include regular periodic overhaul of all the equipment and replacement of equipment which is reaching the end of its serviceable life.
- 7.6.4 The maintenance agreement will also provide for 'emergency' attendance by a specialist CCTV engineer on site to rectify any loss or severe degradation of image or camera control.
- 7.6.5 The maintenance agreement will define the maximum periods of time permitted for attendance by the engineer and for rectification of the problem depending upon the severity of the event and the operational requirements of that element of the system.
- 7.6.7 It is the responsibility of the System Manager to ensure appropriate records are maintained in respect of the functioning of the cameras and the response of the maintenance organisation. As soon as practicable this will be managed electronically.

Section 8 Access to, and Security of, Monitoring Room and Associated Equipment

8.1 Authorised Access

8.1.1 Only trained and authorised personnel (LBHF or Police) will operate any of the equipment located within the CCTV monitoring room, (or equipment associated with the CCTV System). Only staff approved by police under local protocols will be allowed to monitor any police radio or data system fitted in the room. Casual visits by other staff, from whatever department, will not be permitted and procedures will be put in place to ensure these are not necessary.

8.2 Public access

8.2.1 Public access to the monitoring and recording facility will be prohibited except for lawful, proper and sufficient reasons and only then with the personal authority of the system manager. Any such visit will be conducted and recorded in accordance with the Procedures Manual. Any equipment subject of protocols or agreements with partners (police radio or data systems) will be turned off for the duration of any visit. Consideration must be given to the suitability of any images on display during any visit.

8.3 Authorised Visits

8.3.1 Any inspection necessary under statutory legislation will be advised in advance. Inspectors or Auditors will not influence the operation of any part of the system during their visit. The visit will be suspended in the event of it being operationally inconvenient. Any such visit should be recorded in the same way as that described above.

8.4 Declaration of Confidentiality

8.4.1 Regardless of their status, all visitors to the CCTV monitoring room, including inspectors and auditors, will be required to sign the visitor's book and a declaration of confidentiality. Suitable signage will be displayed on entry on the room and by the visitor's book reminding staff of their obligation to maintain confidentiality. Persons who feel unable to sign will be refused entry.

8.5 Security

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

8.5.2 Wherever possible the minimum standards for control room operations set out in BS7499 will be complied with. Access to the room will be through the interlocking pairs of doors which are secured by 'Magnetic-Locks' operated by the CCTV operator. Key pads currently control access and it is intended that a new proximity access control system will be adopted to provide a better degree of security and to maintain a record of access and egress. Use will be made of the intercom and internal camera system to identify callers and maintain the integrity of the security of the room.

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 on videotape or by way of video copying, including still prints and CD -Rom downloads of images.
- 9.1.2 Every video or digital recording obtained by using the System has the potential of containing material that has to be admitted in evidence at some point during its life span. All images, tapes and CD's used remain the property of the LBHF and must not be copied except by police for the purposes of investigations or legal proceedings.
- 9.1.3 Members of the community must have total confidence that information recorded about their ordinary every day activities by virtue of the System, will be treated with due regard to their individual right to respect for their private and family life.
- 9.1.4 It is therefore of the utmost importance that irrespective of the means or format (e.g. paper copy, video tape, digital tape, CD, or any form of electronic processing and storage) of the images obtained from the system, they are treated strictly in accordance with this Code of Practice and the Procedural Manual from the moment they are received by the monitoring room until final destruction. Every 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 of Practice only.
- 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 personal data generated by this CCTV System will be channelled through the System Manager. The System Manager will ensure the principles contained within Appendix C to this Code of Practice 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 individual's rights to privacy and to give effect to the following principles:
- Recorded material shall be processed lawfully and fairly, and used only for the purposes defined in this Code of Practice;
 - Access to recorded material will only take place in accordance with the standards outlined in Appendix C and this Code of Practice;
 - The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.
- 9.2.3 Members of the police service or other agency having a statutory authority to investigate and / or prosecute offences may, subject to compliance with 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. The system manager must be advised prior to the release of such data

Note: Release to the media of recorded information, in whatever format, which may or may not be part of a current investigation would be covered by the Police and Criminal Evidence

Act, 1984 and the Crime Procedure & Investigations Act 1996. Any such disclosure should only be made after due consideration of the likely impact on a criminal trial.

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

9.2.5 It may be beneficial to make use of 'real' video footage for the training and education of those involved in the operation and management of CCTV systems, and for those involved in the investigation, prevention and detection of crime. Any material recorded by virtue of this CCTV system will only be used for such bona fide training and education purposes. Recorded material will not be released for commercial or entertainment purposes.

9.3 Video Tapes - Provision & Quality

9.3.1 To ensure the quality of the tapes, and that recorded information will meet the criteria outlined by current Home Office guidelines, the only video tapes to be used with the system are those which have been specifically provided in accordance with the Procedures Manual.

9.4 Tapes – Retention

9.4.1 Recorded video tapes will be retained for a period of 31 days and digital images for at least 21 days, to allow retrospective evidential searches by police. Before reuse or destruction, each tape will be magnetically erased in full accordance with the manufacturers requirements

9.4.2 This tape retention policy will be notified to the Police and Crown Prosecution Service.

9.4.3 Videotapes will be always be used and stored in accordance with the Procedures Manual. At the conclusion of their life within the CCTV System they will be destroyed and the destruction certified.

9.5 Tape Register

9.5.1 Each tape will have a unique tracking record maintained in accordance with the procedural manual, which will be retained for at least three years, after the tape has been destroyed. The tracking record shall identify every use, and person who has viewed or had access to the tape since the initial breaking of the seal to the destruction of the tape. Similar process will be used in respect of digital recordings. As soon as practicable an electronic method of recording this information will be adopted.

9.6 Recording Policy

9.6.1 Subject to the equipment functioning correctly, images from every camera will be recorded throughout every 24 hour period in 12 hour time lapse mode, through digital multiplexers onto quality VHS video tapes or computer disk. The number of images through each multiplexer (or the time number of frames recorded on a digital system) will be such that the time between successive frames once played back in time lapse mode shall not exceed 2 seconds.

9.6.2 Images from selected cameras will be recorded in real time at the discretion of the CCTV operators or as directed by the System Manager.

9.7 Evidential Tapes

9.7.1 In the event of a tape being required for evidential purposes the procedures outlined in the Procedures Manual will be strictly complied with.

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 Procedures Manual.
- 10.1.3 Video prints contain data and will therefore only be released under the terms of Appendix C to this Code of Practice, 'Release of data to third parties'. If prints are released to the media, (in compliance with Appendix C), in an effort to identify alleged offenders or potential witnesses, full details will be recorded in accordance with the Procedures Manual.
- 10.1.4 A record will be maintained of all video print productions in accordance with the Procedural Manual. The recorded details will include: a sequential number, the date, time and location of the incident, date and time of the production of the print and the identity of the person requesting the print, (if relevant) and the purpose for which the print was taken.
- 10.1.5 The destruction of prints must be recorded in the control room incident log.
- 10.1.6 The records of the video prints taken will be subject to audit in common with all other records in the system.

Appendix A Key Personnel and Responsibilities

1. System Owners

London Borough of Hammersmith & Fulham

The Emergency Planning & Risk Manager

Tel: 020-8753 2260.

Fax: 020-8563 0732.

Room 313

Hammersmith Town Hall

King Street

Hammersmith

London

W6 9JU

Responsibilities:

The London Borough of Hammersmith & Fulham is the 'owner' of the system. The Emergency Planning & Risk Manager will be the single point of reference on behalf of the owners. His/her role will include a responsibility to:

- i) *Ensure the provision and maintenance of all equipment forming part of the London Borough of Hammersmith & Fulham System in accordance with contractual arrangements which the owners may from time to time enter into.*
- ii) *Maintain close liaison with the control room manager.*
- iii) *Ensure the interests of the joint owners and other organisations are upheld in accordance with the terms of this Code of Practice.*
- iv) *Agree to any proposed alterations and additions to the system, this Code of Practice and / or the Procedures Manual.*

2. System Management

London Borough of Hammersmith & Fulham

CCTV Development & Security Adviser

Tel: 020-8753 2286.

Fax: 020-8563 0732.

Room 313

Hammersmith Town Hall

King Street

Hammersmith

London

W6 9JU

Responsibilities:

The CCTV Development & Security Adviser is the 'manager' of the CCTV system. He/She has delegated authority for data control on behalf of the 'data controller'.

Their role includes responsibility to:

- i) Maintain day to day management of the system and liaises with CCTV staff managers;
- ii) Accept overall responsibility for the system and for ensuring that this Code of Practice is complied with;
- iii) Maintain direct liaison with the owners of the system.
- iv) Maintain direct liaison with operating partners.

Appendix B Extracts from Data Protection Act 1998

Section 7

- (1) Subject to the following provisions of this section and to sections 8 and 9, an individual is entitled:
 - (a) to be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller.
 - (b) If that is the case, to be given by the data controller a description of –
 - (i) the personal data of which that individual is the data subject;
 - (ii) the purpose for which they are being or are to be processed;
 - (iii) the recipients or classes of recipients to whom they are or may be disclosed,
 - (c) to have communicated to him/her in an intelligible form:
 - (i) the information constituting any personal data of which that individual is the data subject;
 - (ii) any information available to the data controller as the source of those data;
 - (d) where the processing by automatic means of personal data of which that individual is the data subject for the purposes of evaluating matters relating to him/her such as, for example, his/her performance at work, his/her creditworthiness, his/her reliability or his/her conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him/her, 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/she has received:
 - (a) a request in writing, and
 - (b) except in prescribed cases, such fee (not exceeding the prescribed maximum) as he/she may require.
- (3) A data controller is not obliged to comply with a request under this section unless he/she is supplied with such information as he/she may reasonably require in order to satisfy him/herself 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/she is not obliged to comply with the request unless:
 - (a) the other individual has consented to the disclosure of the information to the person making the request, or
 - (b) it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

- (5) In subsection (4) the reference to information relating to another individual includes a reference to information identifying that individual as the source of the information sought by the request; and that subsection is not to be construed as excusing the data controller from communicating so much of the information sought by the request as can be communicated without disclosing the identity of the other individual concerned, whether by omission of names or other identifying particulars or otherwise.
- (6) In determining for the purposes of subsection (4)(b) whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned, regard shall be had, in particular, to:
- (a) any duty of confidentiality owed to the other individual,
 - (b) any steps taken by the data controller with a view to seeking the consent of the other individual,
 - (c) whether the other individual is capable of giving consent, and
 - (d) any express refusal of consent by the other individual.

Note: *In considering such instances the data controller must effectively also consider the degree of privacy that the third parties might or might not reasonably expect in being at that location at that time.*

- (7) An individual making a request under this section may, in such cases as may be prescribed, specify that his/her 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 forgoing 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/her to comply with the request.

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 the request or, if later, the first day on which the data controller has both the required fee and the information referred to in subsection (3).

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

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

www.informationcommissioner.gov.uk

Section 8

- (1) The Secretary of State may by regulations provide that, in such cases as may be prescribed, a request for information under any provision of subsection (1) of section 7 is to be treated as extending also to information under other provisions of that subsection.
- (2) The obligation imposed by section 7(1)(c)(i) must be complied with by supplying the data subject with a copy of the information in permanent form unless:
 - (a) the supply of such a copy is not possible or would involve disproportionate effort, or
 - (b) the data subject agrees otherwise;
 - (c) and where any of the information referred to in section 7(1)(c)(i) is expressed in terms which are not intelligible without explanation the copy must be accompanied by an explanation of those terms.
- (3) Where a data controller has previously complied with a request made under section 7 by an individual, the data controller is not obliged to comply with a subsequent identical or similar request under that section by that individual unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request.
- (4) In determining for the purposes of subsection (3) whether requests under section 7 are made at reasonable intervals, regard shall be had to the nature of the data, the purpose for which the data are processed and the frequency with which the data are altered.
- (5) Section 7(1)(d) is not to be regarded as requiring the provision of information as to the logic involved in decision-taking if, and to the extent that, the information constitutes a trade secret.
- (6) The information to be supplied pursuant to request under section 7 must be supplied by reference to the data in question at the time when the request is received, except that it may take account of any amendment or deletion made between that time and the time when the information is supplied, being an amendment or deletion that would have been made regardless of the receipt of the request.
- (7) For the purposes of section 7(4) and (5) another individual can be identified from the information being disclosed if he/she can be identified from that information, or from that and any other information which, in the reasonable belief of the data controller, is likely to be in, or to come into, the possession of the data subject making the request.

Appendix C National Standard for the release of 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.

The London Borough of Hammersmith & Fulham and the Metropolitan Police 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 System owners have adopted the nationally recommended standard of The CCTV User Group.

2. General Policy

All requests for the release of data shall be processed in accordance with the Procedures Manual. All such requests shall be channelled through the data controller. Day to day responsibility may be devolved, usually to the scheme manager

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 public enquiries, civil proceedings, tribunals or hearings – internal and external
 - 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 ⁽¹⁾
 - ii) Statutory authorities with powers to prosecute, (e.g. Customs and Excise; Trading Standards, etc.)
 - iii) Solicitors ⁽²⁾
 - iv) Plaintiffs in civil proceedings⁽³⁾
 - v) Accused persons or defendants in criminal proceedings ⁽³⁾

- v) Other agencies, according to purpose and legal status⁽⁴⁾.
- 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.

Note : A time limit could apply providing reasonable notice was issued to the agent, prior to the destruction of the held data, (e.g. a time limit was about to expire).

- 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.
- (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.

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'⁽¹⁾.
- 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⁽²⁾.
 - ii) If the material is to be released under the auspices of 'public well being, health or safety', written agreement to the release of material should be obtained from a senior officer within the Local Authority. The officer should have personal knowledge of the potential benefit to be derived from releasing the material and an understanding of 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.

Note:

- (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

- 1) Under the terms of Data Protection legislation, individual access to personal data, of which that individual is the data subject, must be permitted providing:
 - i) The request is made in writing;
 - ii) 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 requestee 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 that 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 requestee.

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⁽¹⁾.

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.

The CCTV System

I,, am retained by the London Borough of Hammersmith & Fulham to perform the duty of CCTV Operator / Supervisor / Manager / Insert other*. I have received a copy of the Code of Practice in respect of the operation and management of that CCTV System.

I hereby declare that:

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

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

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

Signed: Print Name:

Witness: Position:

Dated this day of (month) 200 ...

*delete / insert where applicable

WARNING

RESTRICTED ACCESS AREA

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

Visitors are advised to note the following confidentiality clause and entry is conditional on acceptance of that clause:

Confidentiality Clause:

'In being permitted entry to this area you acknowledge that the precise location of the CCTV monitoring room is, and should remain, confidential. You agree not to divulge any information obtained, overheard or overseen during your visit. An entry accompanied by your signature in the Visitors book is your acceptance of these terms'.



Memorandum of Understanding**The sharing and exchange of CCTV images in the London Borough of Hammersmith & Fulham****1 Parties**

This Memorandum of Understanding is made between the parties listed in Schedule 1 (hereinafter called "the Partners").

2 Objective

The Partners wish to share and exchange both live and recorded images from their respective close circuit television systems ("CCTV") for the purpose of crime prevention and detection, major incidents and serious hazards.

3 Understanding

This Memorandum of Understanding outlines how the Partners are collectively seeking to achieve the desired Objective.

The Partners undertake as follows:

3.1 Each Partner shall comply **fully** with the provisions of:

- Data Protection Act 1998
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Crime and Disorder Act 1998
- Their own existing CCTV code of practice

3.2 The Partner recording images will remain the Data Controller (as defined in the Data Protection Act 1998) and will hold a notification with the Office of the Information Commissioner.

3.3 Partner(s) receiving images will be the Data Processor (as defined in the Data Protection Act 1998).

3.4 Master tapes will remain in the possession of the Data Controller, unless seized by Police.

3.5 Partners will provide the Police with master tapes in respect of which they are Data Controllers if requested by the Police to do so in the event of evidence being

required in connection with any criminal court proceedings in accordance with their respective codes of practice.

- 3.6 Tape Movement Registers will be maintained separately at each Partner's control centre and will detail full records of viewings, seizures and other relevant information.
- 3.7 Police or its other authorised person or body will be allowed to view images at the nearest control centre. Partners will provide working copies of tapes in respect of which they are Data Controllers if requested to do so by the Police.
- 3.8 Each Partner's CCTV control centre manager will assume responsibility for liaison with the other Partners.
- 3.9 The sharing and exchanging of CCTV images in the London Borough of Hammersmith & Fulham (LBHF) will be incorporated as a standing agenda item on the LBHF CCTV User Group for monitoring, evaluation and problem solving purposes.
- 3.10 All Partners shall disclose CCTV images to each other for the purpose of meeting the desired Objective.
- 3.11 Each Partner shall:
 - Not record the CCTV images it has obtained from another Partner without first obtaining written approval from the Partner who is the Data Controller in relation to those images. In exceptional cases, where recording is deemed necessary by a supervisor of the relevant control room to support the objectives at para 2, the Partner who is the Data Controller must be informed as soon as practicable after the recordings have been made and written authority sought retrospectively.(see last para. Below)
 - Not disclose or provide copies of the CCTV images it has obtained from another Partner to a third partner who is not a Partner without first obtaining written approval from the Partner who is the Data Controller in relation to those CCTV images.
 - take reasonable precautions to preserve the integrity and prevent any corruption or loss of the CCTV images in its possession.
 - erase all CCTV images when requested to do so by the Partner who is the Data Controller in respect of those images.

4 Commencement

This Memorandum of Understanding shall commence on the date when it was duly signed by all the Partners.

5 Changes to the Memorandum of Understanding

All additions, amendments and variations to this Memorandum of Understanding shall be binding only if in writing and signed by a duly authorised representative of each Partner.

6 Counterparts

This Memorandum of Understanding may be executed in one or more counterparts each signed by one or more of the Partners and such counterparts shall together constitute one document.

Signed for and on behalf of:

1 Partner: **London Borough of Hammersmith & Fulham,**
Signature:
Name of Signatory:
Office Held:
Date:

2 Partner: **W12 Shopping Centre**
Signature:
Name of Signatory:
Office Held:
Date:

3 Partner: **Chelsea Football Club**
Signature:
Name of Signatory:
Office Held:
Date:

4 Partner: **Queens Park Rangers Football Club**
Signature:
Name of Signatory:
Office Held:
Date:

5 Partner: **Fulham Broadway Shopping Centre**
Signature:
Name of Signatory:
Office Held:
Date:

6 Partner: **Hammersmith Hospital**
Signature:
Name of Signatory:
Office Held:
Date:

7 Partner: **Charing Cross Hospital**
Signature:
Name of Signatory:
Office Held:
Date:

Schedule 1

Parties to the Memorandum of Understanding

Adrian Price
Emergency Planning & Risk Manager
London Borough of Hammersmith & Fulham
Town Hall
King Street
London
W6 9JU
0208 753 2286
adrian.price@lbhf.gov.uk

W12 Shopping Centre

Fulham Broadway Shopping Centre (Pillars)

Chelsea Football Club

Queens Park Rangers Football Club

Hammersmith Hospital

Charing Cross Hospital

Appendix G Subject Access Request Form

Subject Access Request Form

To enable us to deal with your request as quickly and efficiently as possible, please complete the relevant sections below. Unfortunately we do not have the resources to respond to requests which ask for *everything you hold on me*.

1. Details of Person Requesting the Information

Title:

Full Name:

Maiden/Former Names:

Address (please tell us about previous addresses in question 5):

Postcode:

Telephone No (inc code):

Fax No (inc code):

Email:

Date of Birth:

2. Is the information about you?

YES, I do not require a CCTV search

please supply **2 original documents** to confirm your identity and address.

Yes, I do require a CCTV search

If you require a CCTV search please **DO NOT** send any documents now, but contact the CCTV Officers to make an appointment at the Town Hall where you will need to present these for checking. If you are unable to visit the Town Hall then please send in the documents requested above together with a declaration from a solicitor, Justice of the Peace or person of similar standing confirming your identity and **a passport sized photograph certified by that person.**

If you have previously made a Subject Access Request to the Council, we may still have your details on file, please give the date of your request.....

(please go to question 4)

NO: Are you acting on behalf of the person with their written authority? If so this original authority must be enclosed and proof of their identity and address. (please complete question 3)

3. Details of the person who the information is about (if different from 1)

Title:

Full Name:

Maiden/Former Names:

Address (please tell us about previous addresses in question 5):

Postcode:

CCTV Code of Practice for the London Borough of Hammersmith & Fulham

Telephone No (inc code):

Fax No (inc code):

Email:

Date of Birth:

4. The information you seek.

Please tick all relevant boxes

Housing

Benefits	Leasehold/Right to Buy
Rents	Estates Management
Repairs	Private Housing Conditions
Allocations	Housing Aid
Homeless persons	Tenancy Relations

CCTV (please also complete CCTV Search Form)

Finance

Council Tax (please supply account reference number/s)
Business Rates (please supply account reference number/s)
Payroll (please supply NI no and Pay no.....)
Pensions (please supply NI no and Pay no.....)
Insurance	General Income
Property & Valuation (commercial)	

Social Services

Adults	Children
Mental Health	

Environmental Services

Environmental Health	Trading Standards
Planning	Building Control
Street Services	

Education

For individual educational records, please contact the relevant school

Early years, play and youth	Student awards and benefits
Personnel section	Library Service
School admissions	Adult education and arts
Communications and information team – complaints section	School improvement and pupil inclusion services

Policy and Administration

Shepherds Bush Advice Centre

Direct Services

Parking Services	Enforcement
Leisure Services	Refuse Collection
Recycling	Parks
Graffiti	Borough Highways

Other (please specify).....

5. Please supply any other information which will help us to deal with your request, or which is not already covered.

Fees: Unless you are requesting a CCTV search, we will not charge at this stage – however we reserve the right to do so. Any request for a CCTV search must be accompanied by a cheque or postal order to the value of £10 made payable to the London Borough of Hammersmith & Fulham. Please write Subject Access Request on the back of the cheque.

6. **Declaration:** to be completed by all people seeking information. Please note any attempt to mislead may lead to prosecution.

I.....certify that the information given on this form is true. I understand that it is necessary for the Council to confirm my/ my client’s identity and it may be necessary to obtain more detailed information in order to locate the correct information.

Signature.....

Name (print).....

Date.....

Note: The period of 40 calendar days in which the Council must respond to the request will not commence until it is satisfied upon these matters.

Please return the completed form to:

The Information Manager (responsible for Data Protection)
Legal Services
Town Hall
King Street
Hammersmith
London W6 9JU

Documents which must accompany this application:

- (a) evidence of the individual’s identity who the information is about*
- (b) CCTV search form, recent photograph and payment, if request includes CCTV information*

Completing the Subject Access Request and CCTV Search Form

This first part of this leaflet will tell you how to complete the Subject Access Request Form. The second part will tell you how to complete the supplementary CCTV Search Form.

Subject Access Request Form

Important

It is vital that you complete all the relevant sections as clearly as you can using block capitals. You may also type the information, but you will need to print out this form, sign it and send it back to us.

There are **6** questions on this form.

Question 1 – Details of person requesting the information

Include here the details of the person making the request. This can be the person who the information is about or someone applying on their behalf e.g. a solicitor, social worker, parent or guardian.

You can tell us about previous addresses in Question 5

Question 2 – Is the information about you?

If the answer is **YES** and you **DO NOT** require a CCTV search then we ask you to send 2 original documents to confirm your identity and address.

To prove your **Identity** we are happy to accept

Your birth certificate

Your passport

Solicitor's affidavit confirming your identity

Photo driving licence

To confirm your **Address** we will accept

Paper driving licence

Medical card

National Savings Book

Utility bill (gas, electricity, water, bank statement etc)

Any other official document with your name and address on it

If the answer is YES and you require a CCTV search, DO NOT send any documents now, but contact the CCTV Officers to make an appointment to visit the Town Hall where you will need to present these for checking together with a passport sized photograph.

Contact the CCTV Office by ringing the Council Switchboard on 020 8748 3020

If you are unable to visit the Town Hall, please send a written declaration, ideally on headed paper, from one of the following:

Commissioner of Oaths

Councillor: Local or County

Justice of the Peace

Member of Parliament
Minister of a recognised religion
Officer of the Armed Services (Active or Retired)
Police Officer (serving or retired)

They should confirm that they have checked the documents provided together with the photograph and they must endorse the back of the photograph as follows, "I certify this to be a true likeness of.....(insert subject name)", sign and date it.

If you have previously made a Subject Access Request to the Council, we may still have your details on file. If are able to give us the date of your request, this may help us to locate the information you seek.

If the answer is **NO**, and you are acting on behalf of someone else with their written authority, please enclose this and proof of their identity and address as outlined in Question 2. CCTV requests will only be accepted by the person who the information is about, or by someone from the list above.

Question 3 – Details of the Person who the information is about (if different from 1)

This should be completed if person requesting the information is not the subject of it.

You can tell us about previous addresses in Question 5

Question 4 – The information you seek

Please tick the boxes to indicate the areas of interest.

If you require a CCTV search then you will also need to complete the additional CCTV search form.

Some sections ask you to supply account or reference numbers – if these are available please include the details on the form. Failure to give these details may make it more difficult for us to locate information about you on our systems.

Question 5 – Additional Information

Please use this space to supply any additional information which will help us in our search.

This could include:

- Previous addresses
- Previous postcodes
- Relevant dates you were in touch with the Council
- Name of anyone you dealt with at the Council

Fees: We do not normally charge for providing information, however we reserve the right to do so. If you require a CCTV search then you will be asked to pay.

The maximum we can charge for any request is £10 and we will always tell you if there will be a charge before going any further.

Any request for a CCTV search must be accompanied by a cheque or postal order to the value of £10 made payable to the London Borough of Hammersmith & Fulham. Please write Subject Access Request on the back of the cheque.

Question 6 - Declaration

The person who the information is about or their representative must complete the declaration in full before any application can be considered.

CCTV Search Form

Important

You only need to complete this form if you require information from our CCTV systems. Please note that we delete digital recordings after 21 days and traditional tapes after 31 days.

This is the only section to complete.

Additional Information

This space is for you to give us as much information as possible to enable us to locate the information on our system. You should tell us about your appearance, your clothing, where you were at the time, your vehicle (if relevant), anything else which will help us to identify you on our system.



CCTV Search Form

To enable us to locate personal data about you on our CCTV systems. Please complete this form as fully as possible. Failure to give full details may cause a delay in tracing the information requested or lead to a negative result of the search.

This form should accompany the Subject Access Request Form

Additional Information
Please say whether you are male or female.....
And include FULL location or address, notable landmarks, details of the colour and type of your clothing, details of vehicle if appropriate, any other information which may assist us to identify you or the incident to which you refer.

INTERNAL USE ONLY
Date Application Received.....
Cheque/Postal Order Number.....in the sum of.....
received. Receipt Nosent on.....
LBHF officer signature.....Date.....
Proof of Identity Seen. Type and Number.....
Proof of Address. Type and Number.....
Officer Recording Details (Name/ Ext).....
ENSURE A COPY IS TAKEN OF ALL IDENTIFICATION DOCUMENTS PRODUCED AND PHOTO OF SUBJECT ATTACHED.

Appendix H :- Camera Locations

Cameras are located in the main town centre areas and transport interchanges where the public tell us the fear of crime is highest or the police advise to be a crime hotspot area.

Cameras are located as listed below

Hammersmith - King Street, Glenthorne Road, Hammersmith Broadway and immediate surrounding areas

Fulham - Fulham Broadway, North End Road, New Kings Road and immediate surrounding areas.

Shepherds Bush - Shepherds Bush Green, Uxbridge Road, Goldhawk Road, Melina Road, Wood Lane and immediate surrounding areas.

Appendix I Regulation of Investigatory Powers Act Guiding Principles

Advice and Guidance for Control Room Staff and Police Inspectors in respect of CCTV and the Regulation of Investigatory Powers Act 2000.

The Regulation of Investigatory Powers Act 2000 (RIPA 2000) came into force on 2nd October 2001. It relates to surveillance by the Police and other agencies and deals in part with the use of directed covert surveillance. Section 26 of this act sets out what is Directed Surveillance. It defines this type of surveillance as:-

*Subject to subsection (6), surveillance is directed for the purposes of this Part if it is **covert** but **not intrusive** and is undertaken-*

- (a) for the purposes of a specific investigation or a specific operation;*
- (b) in such a manner as 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*
- (c) 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*

The impact for staff in the Police control rooms and CCTV monitoring centres, is that there might be cause to monitor for some time, a person or premises by using the cameras. In most cases, this will fall into sub section **c** above, i.e. it 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 code says some hours rather than minutes.

In cases where a pre-planned incident or operation wishes to make use of CCTV for such monitoring, an authority will almost certainly be required.

Slow time requests are authorised by a Superintendent or above.

If an authority is required immediately, an Inspector may do so. The forms in both cases must indicate the reason 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.*

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 in writing by way of the form below. Any authority given should be recorded appropriately for later reference. This should include the name of the officer authorising.

Forms are available from the System Manager

Examples:

Insp. Authorisation

An example of a request requiring Inspector authorisation 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 to note who goes to and from the vehicle.

Supt Authorisation

Where crime squad officers wish to have a shop premises monitored from the outside, which is suspected of dealing in stolen goods over a period of days.

No Authorisation

Where officers come across a local drug dealer sitting in the town centre/street and wish to have the cameras monitor them, so as not to divulge the observation taking place.

PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) 2000

CONFIRMATION OF AUTHORISATION TO CARRY OUT DIRECTED SURVEILLANCE

Police Authority <i>(including full address)</i>	
--	--

Name of Applicant		Unit/Branch /BOCU	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
PAT Number:			

Details of application:

1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) Order 2000; No. 2417. ¹

¹ Will usually be a Superintendent or above.

2. Describe the authorised conduct or operation		Describe the purpose of the investigation	
		Vehicle Crime	<input type="checkbox"/>
		Firearms Related Offences	<input type="checkbox"/>
		Drugs Related	<input type="checkbox"/>
		Violence against the Person	<input type="checkbox"/>
		Homicide	<input type="checkbox"/>
		Theft of/From	<input type="checkbox"/>
		Burglary	<input type="checkbox"/>
		Terrorism	<input type="checkbox"/>
		Vehicle Hijack	<input type="checkbox"/>
3. Anticipated Start	Date:	Time	
Duration:			

Confirmation of Authority			
<p>I, _____, hereby confirm that directed surveillance investigation/operation has been authorised as detailed above. This written authorisation will cease to have effect at the end of a period of 3 months unless renewed (see separate form for renewals).</p> <p>This authorisation will be reviewed frequently to assess the need for the authorisation to continue.</p>			
Name (Print)		Grade / Rank	
Signature		Date	

Date of first review:	
Date of subsequent reviews of this authorisation:	

References

The CCTV User Group	<i>Model Code of Practice</i>
HMSO	<i>The Police and Criminal Evidence Act, 1984.</i> HMSO
HMSO	<i>The Police and Criminal Evidence Act 1984, Codes of Practice, April 1995</i>
HMSO	<i>The Criminal Procedures and Investigations Act, 1996</i> HMSO
HMSO	<i>The Data Protection Act, 1998. and</i> <i>CCTV Code of Practice</i>
HMSO	<i>The Human Rights Act, 1998.</i>
HMSO	<i>The Regulation of Investigatory Powers Act 2000</i>
HMSO	<i>Crime and Disorder Act 1998</i>
Home Office	<i>"Looking out for you"</i>
Police Scientific Development Branch	<i>"CCTV Operational Requirements Manual"</i>
British Standards institute	<i>BS EN 50132 Part VII</i>