

The London Borough of Barnet

in partnership with



The Metropolitan Police Barnet Borough Division

Code of Practice for the operation of
Closed Circuit Television

Feb 2009

Change Control

Item	Reason for Change	Version	Author	Date
1	First draft	1.0	Gary Davies	14.05.2003
2	Cameras added	1.1	Gary Davies	06.02.2004
3	Cameras added	1.2	Gary Davies	14.03.2005
4	Cameras added & minor amendments	1.3	Gary Davies	16.06.2006
5	Cameras added	1.4	Gary Davies	02.05.2007
6	Cameras added	1.5	Gary Davies	14.05.2008
7	Cameras added	1.6	Gary Davies	19.02.2009

Code of Practice in Respect of
The Operation of
The London Borough of Barnet
CCTV System

Agreed by

Barnet Council
and
The Metropolitan Police, Barnet Borough Division

Certificate of Agreement

The content of this Code of Practice is hereby approved in respect of the London Borough of Barnet Closed Circuit Television System and, as far as is reasonably practicable, will be complied with by all who are involved in the management and operation of the System.

Signed for and on behalf of the London Borough of Barnet

Signature: ORIGINAL DOCUMENT SIGNED AND DATED

Name: Position held:

Dated the day of 200...

Signed for and on behalf of The Metropolitan Police, Barnet Borough Division

Signature: ORIGINAL DOCUMENT SIGNED AND DATED

Name: Position held:

Dated the day of 200...

1.1 Introduction

A system of Closed Circuit Television (CCTV) has been introduced to the London Borough of Barnet. This system, known as 'Barnet CCTV', comprises a number of cameras installed at strategic locations. All of the cameras are fully operational with pan, tilt and zoom facilities. Images from the cameras are presented in the Council's CCTV Control Room via secure fibre optic links.

Barnet CCTV is able to relay images of selected cameras to the Metropolitan Police Command & Control system to assist with incident response but there are no recording facilities at any location other than the Barnet CCTV monitoring room.

Barnet CCTV also has a covert capability, comprising of a number of small, discreet cameras and associated recording equipment.

Barnet CCTV also includes a vehicle mounted mobile CCTV unit. This unit is equipped with two mast mounted cameras and a remotely deployable camera. All cameras are fully controllable and are monitored and recorded from within the vehicle. The remote camera is also capable of being controlled and monitored from a covert unit away from the main vehicle.

Barnet CCTV has evolved from the formation of a partnership between the London Borough of Barnet and the Metropolitan Police, Barnet Borough Division who have both certified on the previous form their acceptance of the requirements of this code.

For the purposes of this document, the 'owner' of the system is the London Borough of Barnet
For the purposes of the Data Protection Act the 'data controller' is the London Borough of Barnet

The 'System Manager' is the London Borough of Barnet CCTV Manager.

Barnet CCTV has been notified to 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 of the functions of a public service nature are required to observe the obligations imposed by the Human Rights Act 1998, and consider that the use of CCTV in Barnet 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 Metropolitan Police towards their duty under the Crime and Disorder Act 1998.
- 1.2.3 It is recognised that operation of Barnet CCTV may be considered to infringe on the privacy of individuals. The partnership recognises 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.

1.2.5 Barnet CCTV 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 Barnet CCTV, as determined by the owner, which form the lawful basis for the processing of data are: -

- *To help reduce the fear of crime*
- *To help deter crime.*
- *To help reduce vandalism and antisocial behaviour.*
- *To help detect crime and provide evidential material for court proceedings*
- *To assist in the overall management of the London Borough of Barnet*
- *To enhance community safety, assist in developing the economic well being of the London Borough of Barnet and encourage greater use of town centre facilities.*
- *To assist the London Borough of Barnet in its licensing, enforcement and regulatory functions*
- *To assist in traffic management and enforcement*
- *To assist in supporting civil proceedings which will help detect crime*
- *To assist in the training of CCTV operators, the Police and others involved in the use of the CCTV system*

1.4 Procedural Manual

This Code of Practice (hereafter referred to as 'the Code') is supplemented by a separate 'Procedural 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 procedural 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 Barnet CCTV, (hereafter referred to as 'The System') and to outline how it is intended to achieve the objectives detailed within Section 1.

2.2 General Principles of Operation

- 2.2.1 The system will be operated in accordance with all the requirements and the principles of the Human Rights Act 1998.
- 2.2.2 The operation of the system will also recognise the need for formal authorisation of any covert 'Directed' surveillance as required by the Regulation of Investigatory Powers Act 2000 and the Police force 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 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 will remain with the Data Controller.

2.4 Cameras and Area Coverage

- 2.4.1 The areas covered by CCTV to which this Code of Practice refers are the public areas within the London Borough of Barnet or immediately adjacent to it's boundary.
- 2.4.2 From time to time transportable or mobile cameras may be temporarily sited within the area. The use of such cameras, and the data produced by virtue of their use, will always accord with the objectives of the system and be governed by these Codes and Procedures.
- 2.4.3 Most 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 unless such use has been fully assessed and authorised in accordance with 2.2.2 above.
- 2.4.5 A schedule showing the number and location of all fixed cameras is attached at Appendix E to these Codes.

2.5 Monitoring and Recording Facilities

- 2.5.1 A staffed monitoring room is located within the London Borough of Barnet. The CCTV equipment therein has the capability of recording all cameras simultaneously throughout every 24 hour period.
- 2.5.2 Secondary monitoring equipment is located at Colindale Police station. No equipment, other than that housed within the main CCTV control room shall be capable of recording images from any of the fixed cameras listed at Appendix E.
- 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.
- 2.5.4 The mobile CCTV unit, deployable and covert camera systems each incorporate separate monitoring and recording equipment appropriate to their intended use. All monitoring and recording carried out using this equipment shall be in accordance with this Code of Practice.

2.6 Human Resources

- 2.6.1 Unauthorised persons will not have access to the CCTV control room or any associated equipment 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 Procedural 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 technical manual 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 organisations with a participatory role in the operation of the system.
- 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 System Manager and the owners of the system.

3.1 Public Concern

- 3.1.1 Although the majority of the public at large may have become accustomed to 'being watched', those who do express concern do so mainly over matters pertaining to the processing of the information, (or data) i.e. what happens to the material that is obtained.
- 3.1.2 All personal data obtained by virtue of Barnet CCTV 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 Barnet CCTV has been notified to the Office of the Information Commissioner in accordance with current Data Protection legislation.
- 3.2.2 The 'data controller' for Barnet CCTV is the London Borough of Barnet and day to day responsibility for the data will be devolved to the CCTV Manager
- 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 are adequate, relevant and not excessive in relation to the purpose for which the data are held.
 - v) Steps will be taken to ensure that personal data are 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 CCTV Manager or Data Controller.
- 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, those Sections 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 form is included in Appendix D.

3.4 Exemptions to the Provision of Information

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

3.4.1 Personal data processed for any of the following purposes -

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

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

3.5 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 procedural 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 control room is restricted in accordance with this Code of Practice. However, in the interest of openness and accountability, anyone wishing to visit the room may be permitted to do so, subject to the approval of, and after making prior arrangements with, the manager of the System.
- 4.1.2 Cameras will not be used to look into private residential property. Where the equipment permits it 'privacy zones' will be programmed into the system, as required, in order to ensure that the cameras do not survey the interior of any private residential property within range of the system. 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 Barnet CCTV may do so by contacting the council's Customer Care Unit. All complaints shall be dealt with in accordance with the London Borough of Barnet complaints procedure, details of which may be obtained at any Action Point or at www.barnet.gov.uk. Any performance issues identified will be considered under the organisations disciplinary procedures to which all members of the London Borough of Barnet, 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 Manager

- 4.2.1 The nominated manager indicated at appendix A will have day-to-day responsibility for the system as a whole.
- 4.2.2 The system will be subject to annual audit by the Chief Street Services Manager (or nominated deputy whose organisational level of responsibility is at least equal to that of the System Manager, but who is not the System Manager).
- 4.2.3 The System Manager will ensure that every complaint is acknowledged in writing within 15 working days, which will include advice to the complainant of the enquiry procedure to be undertaken. A formal report will be forwarded to the Customer Care Unit giving details of all complaints and the outcome of relevant enquiries.
- 4.2.4 Statistical and other relevant information, including any complaints made, will be included in the Annual Reports of the London Borough of Barnet, which are made publicly available.

4.3 Public Information

4.3.1 Code of Practice

A copy of this Code of Practice shall be published on the London Borough of Barnet website and a printed copy will be made available to anyone on request.

4.3.2 Annual Report

The annual report and that for subsequent years shall be published by the end of June in the year following the reporting year. A copy of the annual report will also be made available to anyone requesting it. Additional copies will be lodged at public libraries, the Town Hall and Barnet House.

4.3.3 Signs

Signs will be placed at main entrance points to the areas under CCTV surveillance. The signs will indicate:

- The presence of CCTV monitoring;
- The 'ownership' of the system;
- Contact telephone number of the 'data controller' of the system.

An example of the current signage is shown below.



4.3.4 Exemptions

In exceptional and limited cases, where it is assessed that the use of signs would not be appropriate, cameras will not be deployed until:

- a) Specific criminal activity has been identified.
- b) The need to use surveillance to obtain evidence of that criminal activity has been identified.
- c) An assessment has been made as to whether the use of signs would prejudice success in obtaining such evidence.
- d) An assessment has been made as to how long the covert monitoring should take place, to ensure that it is not carried out for longer than is necessary.
- e) The information relating to (a) to (d) above has been clearly documented.

Section 5 Assessment of the System and Code of Practice

5.1 Evaluation

5.1.1 Barnet CCTV will periodically be independently evaluated to establish whether the purposes of the system are being complied with and whether objectives are being achieved. The format of the evaluation shall comply with best practice and be based on assessment of the inputs, the outputs, the process and the impact of the scheme.

- *An assessment of the impact upon crime: This assessment shall include not only the immediate area covered by the cameras but the wider town area, the Police Divisional and regional areas and national trends.*
- *An assessment of the incidents monitored by the system*
- *An assessment of the impact on town centre business*
- *An assessment of neighbouring areas without CCTV*
- *The views and opinions of the public*
- *The operation of the Code of Practice*
- *Whether the purposes for which the system was established are still relevant*
- *Cost effectiveness*

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 five 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 Chief Street Services Manager or his/her nominated deputy, 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 the monitoring room records, videotape histories and the content of recorded material.

5.4 Inspection

5.4.1 A body of individuals who have no direct contact or relationship with the operation of the system may be appointed to be responsible for inspecting the operation of the system.

5.4.1 Inspections should take place at least six times per calendar year by no more than two people at any one time. The inspectors will be permitted access to the CCTV monitoring room, with reasonable prior notice and to the records held therein at any time, provided their presence does not disrupt the operational functioning of the room. Their findings will be reported to the Chief Street Services Manager and their visit recorded in the CCTV monitoring room.

5.4.2 Inspectors will be required to sign a declaration of confidentiality.

Section 6 Human Resources

6.1 Staffing of the Control Room and those responsible for the operation of Barnet CCTV

- 6.1.1 The CCTV Control Room will be staffed in accordance with the procedural manual. Equipment associated with the System will only be operated by authorised personnel who will have been properly trained in its use and all control 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, will be required to sign a confirmation that they fully understand the obligations adherence to these documents places upon them and that any breach will be considered as a disciplinary offence. They will be fully conversant with the contents of both documents, which may be updated from time to time, and which he/she will be expected to comply with so far as is reasonably practicable at all times.
- 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 Barnet CCTV will be subject to the London Borough of Barnet discipline code. Any breach of this Code of Practice or of any aspect of confidentiality will be dealt with in accordance with those discipline rules.
- 6.2.2 The System Manager will accept primary responsibility for ensuring there is no breach of security and that the Code of Practice is complied with. He/she has day-to-day responsibility for the management of the room and for enforcing the discipline rules. 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.

7.1 Guiding Principles

- 7.1.1 Any person operating the cameras will act with utmost probity at all times.
- 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.
- 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 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 No secondary control or recording facilities are installed.

7.4 Operational Command of the System by the Police

- 7.4.1 Under rare and extreme operational circumstances the Police may make a request to command the use of Barnet CCTV. These circumstances may be a major incident or event that has a significant impact on the prevention and detection of crime or public safety. Such use will provide the Police with a broad overview of events in order to command the incident.
- 7.4.2 Applications will be considered on the written request of a Police officer not below the rank of Superintendent. Any such request will only be accommodated upon the personal written permission of an officer of the London Borough of Barnet not below the level of Director.
- 7.4.3 In the event of such a request being permitted, the CCTV Control Room will continue to be staffed, and equipment operated by, only those personnel who are specifically trained to do so, and who fall within the terms of Sections 6 and 7 of this Code. They will then operate under the command of the Police officer designated in the written request, taking into account their responsibilities under this code.
- 7.4.4 In very extreme circumstances a request may be made for the Police to take total control of The System in its entirety, including the staffing of the monitoring room and personal control of all associated equipment, to the exclusion of all representatives of the System owners. Any such request should be made to the System Manager in the first instance, who will consult with the Chief Executive of the London Borough of Barnet. A request for total exclusive control must be made in writing by a Police officer not below the rank of Deputy Assistant Commissioner or person of equal standing.
- 7.4.5 Where such operational requirements arise from an emergency situation and the production of written requests and authorities would result in unacceptable delay, verbal requests and authorisations may be given in accordance with the above.

7.5 Maintenance of the system

- 7.5.1 To ensure compliance with the Information Commissioner's Code of Practice and that images recorded continue to be of appropriate evidential quality, Barnet CCTV shall be maintained in accordance with the requirements of the Procedural Manual under a maintenance agreement.

- 7.5.2 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.
- 7.5.3 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.
- 7.5.4 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.
- 7.5.5 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.
- 7.5.6 It is the responsibility of the System Manager to ensure appropriate records are maintained in respect of the functioning of the cameras and the response of the maintenance organisation.

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

8.1 Authorised Access

8.1.1 Only trained and authorised personnel will operate any of the equipment located within the CCTV control room, (or equipment associated with the CCTV System).

8.2 Public access

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

8.3 Authorised Visits

8.3.1 Visits by inspectors or auditors do not fall into the scope of the above paragraph and may take place at any time, without prior warning. No more than two inspectors or auditors will visit at any one time. 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 control room, including inspectors and auditors, will be required to sign the visitors' book and a declaration of confidentiality. London Borough of Barnet staff deemed by the System Manager to have legitimate reason for regular visits to the CCTV Control Room will sign a confidentiality statement to be retained on file.

8.5 Security

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

8.5.2 The CCTV control room will at all times be secured by electronic locks requiring a swipe card or numeric code entry for access, or by other equally secure means. Doors so secured shall remain closed at all times.

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 Barnet CCTV, but specifically includes images recorded digitally, or on videotape or by way of video copying, including video prints.
- 9.1.2 Every video or digital recording obtained by using Barnet CCTV has the potential of containing material that has to be admitted in evidence at some point during its life span.
- 9.1.3 Members of the community must have total confidence that information recorded about their ordinary every day activities by virtue of Barnet CCTV, 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.
- 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 Information will be made available for traffic and transport monitoring, management and information purposes.
- 9.1.7 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 or, in his absence, a nominated deputy. 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.
- 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 Procedural 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 Recording media - Provision & Quality

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

9.4 Recorded data – Retention

9.4.1 Recorded data will be retained for a period not exceeding one calendar month.

9.4.2 Storage media will be always be used and stored in accordance with the Procedural Manual. Before reuse or destruction, videotapes will be magnetically erased in full accordance with the manufacturer's requirements. At the conclusion of their life within the CCTV System all storage media will be destroyed.

9.5 Storage media Register

9.5.1 Each tape, CD or DVD will have a unique tracking record maintained in accordance with the procedural manual, which will be retained for at least three years after the media has been destroyed. The tracking record shall identify every use, and person who has viewed or had access to the media since the initial breaking of the seal to the destruction of the media

9.6 Recording Policy

9.6.1 Subject to the equipment functioning correctly, images from every camera will be recorded onto computer disk. Recording will normally be at the rate of 2 frames per second.

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 data

9.7.1 In the event of data being required for evidential purposes the procedures outlined in the Procedural Manual will be strictly complied with. Master and working copies of media will be passed to the Police or other investigatory body concerned. Evidential media will not normally be stored within the CCTV Control Room

10.1 Guiding Principles

- 10.1.1 A video print is a copy of an image or images which already exist on videotape, CD, DVD or computer disc. Such prints are equally within the definitions of 'data' and recorded material
- 10.1.2 Video prints will not be taken as a matter of routine. Each time a print is made it must be capable of justification by the originator who will be responsible for recording the full circumstances under which the print is taken in accordance with the Procedural Manual.
- 10.1.3 Video prints contain data and will therefore only be 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 Procedural Manual.
- 10.1.4 A record will be maintained of all video print productions in accordance with the Procedural Manual. The recorded details will include: a sequential number, the date, time and location of the incident, date and time of the production of the print and the identity of the person requesting the print, (if relevant) and the purpose for which the print was taken.
- 10.1.5 The records of the video prints taken will be subject to audit in common with all other records in the system.

Appendix A Key Personnel and Responsibilities

1. System Owner

The London Borough of Barnet
Hendon Town Hall
London NW4 4BG

Telephone: 020 8359 2000

Responsibilities:

- Ensure the provision and maintenance of all equipment forming part of Barnet CCTV in accordance with contractual arrangements.
- Maintain close liaison with the CCTV manager.
- Ensure the interests of the partner organisations are upheld in accordance with the terms of this Code of Practice.
- Agree to any proposed alterations and additions to the system, this Code of Practice and / or the Procedural Manual.

2. System Management

The CCTV Manager
The London Borough of Barnet
Hendon Town Hall
London NW4 4BG

Telephone: 020 8359 2000

Responsibilities:

The CCTV Manager is the 'manager' of Barnet CCTV

He/she has delegated authority for data control on behalf of the 'data controller'.

His/her role includes responsibility to:

- Maintain day-to-day management of the system and staff;
- Accept overall responsibility for the system and for ensuring that this Code of Practice is complied with;
- Maintain direct liaison with the owners of the system.
- 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.
- (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.

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

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

2. General Policy

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

3. Primary Request To View Data

- a) Primary requests to view data generated by a CCTV System are likely to be made by third parties for any one or more of the following purposes:
 - i) Providing evidence in criminal proceedings (e.g. Police and Criminal Evidence Act 1984, Criminal Procedures & Investigations Act 1996, etc.);
 - ii) Providing evidence in civil proceedings or tribunals
 - iii) The prevention of crime
 - iv) The investigation and detection of crime (may include identification of offenders)
 - v) Identification of witnesses
- b) Third parties, which are required to show adequate grounds for disclosure of data within the above criteria, may include, but are not limited to:
 - i) Police ⁽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⁾
 - ii) Other agencies, (which should be specified in the Code of Practice) 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.
- 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. A search request should specify reasonable accuracy (could be specified to the nearest ½ hour)

4. Secondary Request To View Data

- a) A 'secondary' request for access to data may be defined as any request being made which does not fall into the category of a primary request. Before complying with a secondary request, the data controller shall ensure that:
 - i) The request does not contravene, and that compliance with the request would not breach, current relevant legislation, (e.g. Data Protection Act 1998, Human Rights Act 1998, section 163 Criminal Justice and Public Order Act 1994, etc.);
 - ii) Any legislative requirements have been complied with, (e.g. the requirements of the Data Protection Act 1998);
 - iii) Due regard has been taken of any known case law (current or past) which may be relevant, (e.g. R v Brentwood BC ex p. Peck) and
 - iv) The request would pass a test of 'disclosure in the public interest'⁽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.

Notes:

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

5. Individual Subject Access under Data Protection legislation

- 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;
- iii) 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 which is specific to the search request shall be shown.
- d) It must not be possible to identify any other individual from the information being shown, (any such information will be blanked-out, either by means of electronic screening or manual editing on the monitor screen).
- e) If a copy of the material is requested and there is no on-site means of editing out other personal data, then the material shall be sent to an editing house for processing prior to being sent to the 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 following:

- 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.

Appendix D Subject Access Request Form

London Borough of Barnet CCTV System Data Protection Act, 1998

How to Apply For Access To Information Held On the CCTV System

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

Your Rights

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

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

Barnet Council's Rights

The London Borough of Barnet may deny access to information where the Act allows. The main exemptions in relation to information held on the CCTV System are where the information may be held for:

- Prevention and detection of crime
- Apprehension and prosecution of offenders

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

Fee

A fee of £10 is payable for each access request, which must be in pounds sterling. Cheques, Postal Orders, etc. should be made payable to 'The London Borough of Barnet'.

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

- Section 1** Asks you to give information about yourself that will help the Council to confirm your identity. The London Borough of Barnet has a duty to ensure that information it holds is secure and it must be satisfied that you are who you say you are.
- Section 2** Asks you to provide evidence of your identity by producing TWO official documents (which between them clearly show your name, date of birth and current address) together with a recent full-face photograph of you.
- Section 3** Asks you to confirm whether you will accept just viewing the information, or if you want a copy of the information.
- Section 4** **You must sign the declaration**

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

THE CCTV MANAGER, HENDON TOWN HALL, LONDON, NW4 4BG
or hand it in to any main Barnet Council building.

BARNET CCTV SURVEILLANCE SYSTEM
Data Protection Act 1998

SECTION 1 About Yourself

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

PLEASE USE BLOCK LETTERS

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

Your Current Home Address (to which we will reply)								
	PostCode							
A telephone number will be helpful in case you need to be contacted.	Tel. No.							

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

Previous address(es)								
Dates of occupancy	From:				To:			
Dates of occupancy	From:				To:			

BARNET CCTV SURVEILLANCE SYSTEM
Data Protection Act, 1998

SECTION 2 Proof of Identity

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

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

Also a recent, full face photograph of yourself.

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

SECTION 3 Supply of Information

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

- | | |
|---|--|
| (a) View the information and receive a permanent copy | <input type="checkbox"/> YES / <input type="checkbox"/> NO |
| (b) Only view the information | <input type="checkbox"/> YES / <input type="checkbox"/> NO |

SECTION 4 Declaration

DECLARATION (to be signed by the applicant)

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

Signed by

Date

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

NOW – please complete Section 4 and then check the ‘CHECK’ box before returning the form.

BARNET CCTV SURVEILLANCE SYSTEM
Data Protection Act, 1998

SECTION 5 *To Help us Find the Information*

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

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

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

Were you: (tick box below)

A person reporting an offence or incident	<input type="checkbox"/>
A witness to an offence or incident	<input type="checkbox"/>
A victim of an offence	<input type="checkbox"/>
A person accused or convicted of an offence	<input type="checkbox"/>
Other – please explain	<input type="text"/>

<i>Date(s) and time(s) of incident</i>	<input type="text"/>
<i>Place incident happened</i>	<input type="text"/>
	<input type="text"/>
<i>Brief details of incident</i>	<input type="text"/>
	<input type="text"/>
	<input type="text"/>

BARNET CCTV SURVEILLANCE SYSTEM
Data Protection Act, 1998

Before returning this form

- Have you completed ALL Sections in this form?

Please check:

- Have you enclosed TWO identification documents?
- Have you signed and dated the form?
- Have you enclosed the £10.00 (ten pound) fee?

Further Information:

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

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

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

OFFICIAL USE ONLY

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

Application checked and legible?

Date Application Received

Identification documents checked?

Fee Paid

Details of 2 Documents (see page 3)

Method of Payment

Receipt No.

Documents Returned?

Member of Staff completing this Section:

Name

Location

Signature

Date

Appendix E Schedule of Camera Locations

Camera No.	Tally Ho Zone
TH1	High Road j/w Woodhouse Road
TH2	Kingsway j/w Ballards Lane
TH3	High Road j/w Nether Street
TH4	Ballards Lane j/w Nether Street
TH5	High Road outside Tally Ho Pub
TH6	Stanhope Road opposite Car Park
TH7	High Road opposite Percy Road
TH8	Lodge Lane car park
TH9	High Road opposite j/w Torrington Park
TH10	High Road j/w Woodside Park Road
TH11	High Road opposite Avenue Road
TH12	Woodhouse Road opp Lambert Way
Camera No	Edgware Zone
E13	High Street j/w Whitchurch Lane
E14	Station Road j/w Garden City
E15	Station Road j/w Manor Park Gardens
E16	Station Road outside Abbey National
E17	Bakery Path
E18	Station Road j/w Penhurst Gardens
E19	Church Way adj to Edgware Infant School
E139	Glengall Road j/w Marlborough Avenue
Camera No	Golders Green Zone
GG20	Finchley Road j/w Golders Green Road
GG21	Golders Green Road opposite Warman-freed Chemist
GG22	Golders Green Road j/w Armitage Road

GG23	Golders Green Road opposite Powis Gardens
GG24	Finchley Road j/w Helenslea Avenue
Camera No	Grahame Park Estate Zone
GP25	Grahame Park Concourse - South
GP26	Grahame Park Concourse - North
GP27	Quakers Course opposite Bus Stand
Camera No	Childs Hill Zone
CH28	Lower Car Park opposite Garth House
CH29	Templewood Point car park
CH30	Harpenmead Point car park
CH31	Granville Point car park
Camera No	A5 (TfL bus lane) Zone
TFL54	A5 Cricklewood Roadway j/w Depot Approach
TFL56	A5 Cricklewood Broadway opp j/w Mora Road
TFL49	A5 West Hendon Broadway j/w Milton Road
TFL50	A5 West Hendon Broadway j/w Station Road
TFL51	A5 West Hendon Broadway opp j/w Herbert Road
TFL52	A5 West Hendon Broadway opp j/w Borthwick Road
TFL53	A5 The Hyde opp Halfords & Comet superstores
TFL55	A5 The Hyde j/w Colindale Avenue
TFL35	A5 Burnt Oak Broadway j/w Barnfield Road
Camera No	Hendon Zone
H82	Watford Way o/s underground station
H32	Watford Way j/w Station Road
H108	Church Road j/w The Burroughs
H109	Church Road j/w Sunny Gardens Road
H110	Parson Street j/w Finchley Lane
H111	Brent Street opp Brampton Grove

H112	Brent Street opp Bell Lane
H113	Queens Road j/w West View footpath
Camera No	East Barnet Zone
EB42	East Barnet Rd j/w Middle Rd
EB43	Church Hill Rd j/w East Barnet Rd
EB44	Cat Hill j/w Brookside Road
EB45	Church Hill Road car park entrance
EB46	Church Hill Road car park – by footpath
EB47	Church Hill Road opposite car park
EB48	Church Hill Road car park service road
Camera No	Hampden Square Zone
HS40	East side of roundabout
HS41	East side of roundabout
Camera No	High Barnet Zone
HB57	Great North Road j/w Station Road
HB58	Barnet Hill j/w Underhill
HB59	High Street j/w Meadway
HB60	High Street j/w Normandy Avenue
HB61	Fitzjohn Avenue car park
HB62	High Street opp Fitzjohn Avenue
HB63	High Street j/w Wood Street
HB64	High Street j/w Church Passage
HB65	Victors Way by car park
HB66	High Street opp j/w Salisbury Road
HB67	High Street j/w St Albans Road
HB68	Stapylton Road car park
Camera No	Burnt Oak Zone
BO69	Burnt Oak Broadway opp Stag Lane

BO70	Watling Avenue j/w Market Lane
BO71	Watling Avenue j/w Barnfield Road
BO72	Barnfield Road car park
BO73	Watling Avenue o/s station
BO74	Watling Avenue j/w Gervase Road
BO75	Watling Park
BO127	Montrose Park
BO128	Montrose Avenue j/w The Greenway
BO129	Lanacre Avenue j/w Angus Gardens
BO130	Orange Hill Road j/w Littlefield Road
BO131	Orange Hill Road / Abbotts Road
BO132	o/s 225 Deansbrook Road
Camera No	Cricklewood Zone
C76	Cricklewood Broadway j/w Yew Grove
C77	o/s 1 Cricklewood Lane
C78	Cricklewood Lane opp Elm Grove
C79	Cricklewood Lane j/w Lichfield Road
Camera No	Friary Park Zone
FP80	Friary House by bowling green
FP81	Friary House by playground
Camera No	Claremont Way Industrial Estate Zone
CW38	Adj to Unit 4
Camera No	Apex Corner (A1 j/w A41) Zone
AX87	South East footway
AX88	Subway intersection
AX89	North West footway
AX90	North East footway
Camera No	Mill Hill Zone

MH91	The Broadway j/w Hartley Avenue
MH92	The Broadway o/s 65/67
MH93	The Broadway j/w Brockenhurst Gardens
MH94	The Broadway opp Station Road
MH95	Bunns Lane – in station car park
Camera No	New Barnet Zone
NB96	East Barnet Road j/w Brookhill Road
NB97	East Barnet Road j/w Warwick Close
NB98	East Barnet Road j/w Margaret Road
NB99	East Barnet Road opp Sainsbury's
NB100	East Barnet Road j/w Victoria Road & Albert Road
Camera No	Finchley Central Zone
FC101	Ballards Lane j/w Wentworth Park
FC102	Ballards Lane j/w Long Lane
FC103	Ballards Lane j/w Falkland Avenue
FC104	Ballards Lane j/w Redbourne Avenue
FC105	Popes Drive rear of Tesco's
FC106	Ballards Lane opp j/w Nether Street
FC107	Regents Park Road j/w Hendon Lane
Camera No	East Finchley Zone
EF114	High Road j/w Park Road
EF115	High Road j/w Hertford Road
EF116	High Road j/w Kitchener Road
EF117	High Road j/w Beresford Road
EF118	High Road j/w Fortis Green
EF119	High Road j/w Diploma Avenue
EF120	High Road opp East Finchley Underground Station
EF121	East End Road j/w Ossulton Way

Camera No	Whetstone Zone
W122	High Road j/w Oakleigh Road North
W123	Totteridge Lane opp Allum Way
W124	High Road o/s HSBC Bank
W125	High Road j/w Chandos Avenue
Camera No	Mutton Brook Zone
MB133	A406 over Mutton Brook (West)
MB134	A406 over Mutton Brook (East)
MB135	Mutton Brook footpath under A406 (West)
MB136	Mutton Brook footpath under A406 (East)
Camera No	Colindale Zone
CD137	A5 j/w Woodfield Avenue
CD138	A5 j/w Sheaveshill Avenue

Appendix F Regulation of Investigatory Powers Act

Guiding Principles

Introduction

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

The guidance contained in this Code of Practice serves to explain and highlight the legislation to be considered. Comprehensive guidance may be obtained in the Covert Surveillance Code of Practice issued by the home office and available online at www.homeoffice.gov.uk. A copy of this code is to be held in the CCTV Control Room.

Background

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

Neither do the provisions of the Act cover the normal, everyday use of **overt** CCTV surveillance systems. Members of the public are aware that such systems are in use, for their own protection, and to prevent crime. *However*, it had not been envisaged how much the Act would impact on specific, targeted use of public/private CCTV systems by 'relevant Public Authorities' covered in Schedule 1: Part1 of the Act, when used during their planned investigations.

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

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

"Covert surveillance" defined

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

Part II - Surveillance types

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

“Intrusive” surveillance

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

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

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

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

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

Cameras will not be used to look into private residential property. Where the equipment permits it 'Privacy zones' will be programmed into the system as required in order to ensure that the interior of any private residential property within range of the system is not surveyed by the cameras. If such 'zones' cannot be programmed the operators will be specifically trained in privacy issues.

“Directed” surveillance

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

The act says:

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

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

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

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

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

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

Authorisations:

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

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

A Local Authority (within the meaning of section 1 of the Local Government Act 1999).

The prescribed office as a minimum level of authority is:

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

Police Forces - A Police force maintained under section 2 of the Police Act 1996 (Police forces in England and Wales).

- The prescribed level is a Superintendent; for urgent cases an Inspector.

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

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

The ‘authority’ must indicate the reasons and should fall within one of the following categories:-

An authorisation is necessary on grounds falling within this subsection if it is necessary-

(a) in the interests of national security;

(b) for the purpose of preventing or detecting crime or of preventing disorder;

(c) in the interests of the economic well-being of the United Kingdom;

(d) in the interests of public safety;

(e) for the purpose of protecting public health;

(f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or

(g) for any purpose (not falling within paragraphs (a) to (f)) which is specified for the purposes of this subsection by an order made by the Secretary of State.

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

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

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

Forms should be available at each CCTV monitoring centre and are to be included in the procedural manual and available from the CCTV User Group Website

Policing examples:

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

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

Supt Authorisation – non-urgent request

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

No authorisation required

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



This Code of Practice has been based on The CCTV User Group Model Code of Practice, which in turn was compiled using elements of good practice from across the country. It should be used in addition to the Data Protection Act 1998 - Code of Practice for CCTV which provides standards to be met to ensure compliance with that act and the Codes of Practice issued under The Criminal Procedures & Investigations Act 1996; Police & Criminal Evidence Act 1976 and Regulation of Investigatory Powers Act 2000. Any court or tribunal will only recognise Codes of Practice issued under specific legislation.