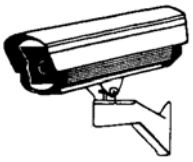


Ealing Council's

A Code of Practice

For the Management of

Closed Circuit Television

"making a difference together"

October 2009

Ealing Council
Perceval House, 14/16 Uxbridge Road, London, W5 2HL
Tel: 020 8825 5000

Preface

Since its introduction to retailers in 1967 and to a town centre in 1985, the use of Closed Circuit Television (CCTV) across the UK has become increasingly popular. 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 peoples' liberty.

Despite the rapid growth of CCTV systems there remains a dearth of statutory regulation governing the use of CCTV cameras. However, 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.

Ealing Council is committed to the belief that everyone has the right to respect for his or her private and family life and their home. This Code of Practice, in conjunction with the Operators Manual, is intended as far as reasonably practicable, to safeguard the integrity of Ealing Council's CCTV Scheme, whilst ensuring the right to privacy is not breached. Both have been updated to ensure compliance with current legislation.

Whilst the contents of this Code of Practice are thought to be accurate at the time of publication, differences and alterations to laws of evidence and procedural matters will inevitably arise. The contents of this document are not intended to form a contract.

Contents

London Borough of Ealing CCTV Code of Practice

Certificate of Agreement

The contents of this Code of Practice is hereby approved in respect of Ealing Council's Closed Circuit Television Scheme and, as far as reasonably practicable, will be complied with by all who are involved in the management and operation of the Scheme.

Signed for and on behalf of: Ealing Council

Signature: …… Name: ……

Position held: ……

Dated the …… day of ……..2009

Signed for and on behalf of: The Metropolitan Police

Signature: …… Name: ……

Position held: ……

Dated the …… day of ……..2009

"making a difference together"

Section 1

Introduction and Objectives

I Introduction

Ealing Council in partnership with the Metropolitan Police is committed to installing and maintaining comprehensive Closed Circuit Television (CCTV) systems throughout the Borough. The installation of each public area CCTV system will contribute to the scheme, which is known as 'Ealing Council's CCTV Scheme'. The Scheme will be monitored and recorded from a central control room. Secondary monitoring and control facilities may be located at other locations (e.g. police control room and housing schemes, *but there are no recording facilities at any location other than the central control room.).*

Ealing Council's CCTV Scheme has evolved from the formation of a partnership between the Metropolitan Police, and a number of external establishments, the local communities and the Council. For the purposes of this document, the 'owner' of the system is the 'Council' and therefore the 'data controller' (1) is the 'Chief Executive'. Details of key personnel, their responsibilities and contact points are shown at appendix A to this Code.

II Aim of the Scheme

The aim of the scheme is:

"To provide a safe public environment for the benefit of those who live, trade, visit and enjoy the facilities of Ealing Council".

III Statement of Purpose

The Statement of Purpose is:

'To install, maintain and monitor a high quality CCTV Scheme in Ealing Council. To utilise this Scheme to safeguard people, their property and the environment, to reduce crime and the fear of crime. With the aim of making the Borough of Ealing an environment in which people can safely use the facilities provided. The statement of purpose is mirrored in the objectives'.

Some of the main objectives of the CCTV Scheme are;

- *To help reduce the fear of crime*
- *To help deter, detect and reduce criminal activities*
- *To assist in aspects of the Council 's management and development strategies for the Borough*
- *To prevent and reduce anti-social behaviour*
- *To assist in the prosecution of offenders*
- *To assist in the better deployment of the Police, Council and other public resources*
- *To enhance community safety*
- *To assist the Local Authority in its enforcement and regulatory functions*
- *To assist with traffic management*
- *To assist in supporting civil proceedings*
- *To comply with this Code of Practice*

IV Procedural Manual

This Code of Practice will be supplemented by a separate Procedural Manual, which details instructions on all aspects of the operation of the system. To ensure the purpose and principles (see Section 2) of the CCTV system are realised, the manual is based upon the contents of this Code of Practice.

Notes:

(1) *The **data controller** is the person who (either alone or jointly or in common with other persons) determines the purpose for which and the manner in which any personal data are, or are to be processed.*

Section 2

Statement of Purpose and Principles

I Purpose

The purpose of this document is to state the intention of both the owner and the manager, on behalf of the partnership as a whole and as far as is reasonably practicable, to support the objectives of Ealing Council's CCTV Scheme, (hereafter referred to as 'The Scheme') and to outline how it is intended to do so.

II General Principles

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

b. The scheme 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.

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

d. Throughout this Code of Practice it is intended, as far as reasonably possible, to offer a balance between the objectives of the CCTV Scheme and the need to safeguard the individual's right to privacy. Throughout the Code every effort has been made to indicate that a formal structure has been put in place, (including a complaints procedure) by which it should be identified that the System is not only accountable, but is seen to be accountable.

e. Participation in the system by any local organization, 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.

III Copyright

Copyright and ownership of all material recorded by virtue of Ealing Council's CCTV Scheme will remain with the Data Controller.

IV Cameras and Area Coverage

The areas covered by CCTV to which this Code of Practice refers are, the London Borough of Ealing. *(e.g. the town centres, housing estates, & industrial estates etc.).* 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 CCTV System. 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. None of the cameras forming part of the Scheme will be installed in a covert manner **(1)**.

V Monitoring and Recording Facilities

a. A fully staffed control room is located at Ealing Town Hall. The CCTV equipment has the capability of recording all cameras simultaneously throughout every 24-hour period.

b. Secondary monitoring equipment is located at Hendon Metcall Communications Centre and some of the housing schemes. *(However, no equipment, other than that housed within the control centre has the capability to record images from any of the cameras)* **(2)**.

c. CCTV operators are able to record images from selected cameras in real time, produce hard copies of recorded images, replay or copy any prerecorded data at their discretion and in accordance with the Code of Practice.

VI Human Resources

Authorised persons will normally always be present whenever the monitoring equipment is in use.

VII Processing and Handling of Recorded Material

All recorded material, whether recorded digitally, in analogue format or as a hard copy video print, will be processed **(3)** and handled strictly in accordance with this Code of Practice and the Procedural Manual.

VIII Operators Instructions

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

IX Changes to the Code of Practice or the Procedural Manual

a. 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 all relevant interested groups, ..

b. 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 owner of the system.

Notes:

(1) *The installation of a CCTV camera is considered to be overt unless it is installed in a manner whereby its presence is deliberately intended to be concealed from the view of any person likely to be within the field of view of that camera.*

Cameras, which may be placed in domes or covered to reduce the likelihood of assessing their field of view, or to protect them from weather or damage, would not be regarded as covert provided that appropriate signs indicating the use of such cameras are displayed in the vicinity.

'Dummy' cameras will not be used as part of the scheme.

(2) *Although catered for within this Code, it is strongly recommended that the recording of images should not, unless unavoidable, take place at more than one location.*

(3) *It should be noted that, under the terms of the Data Protection Act 1998, 'Processing' includes the actual obtaining of data. It is recommended that the same definition should be applied to the processing of data gathered by virtue of a CCTV System, whether or not it is registered under Data Protection legislation. The definition, in full, is reproduced as follows:*

> *'Processing', in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:*
>
> a. *Organization, adaptation or alteration of the information or data,*
>
> b. *Retrieval, consultation or use of the information or data,*
>
> c. *Disclosure of the information or data by transmission, dissemination or otherwise making available, or*
>
> d. *Alignment, combination, blocking, erasure or destruction of the information or data.*

Section 3

Privacy and Data Protection

I Public Concern

a. Consultation and public surveys have shown that the majority of the public at large, support and have become accustomed to CCTV, 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.

NB: ***'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. organization, 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.

b. All personal data obtained by virtue of Ealing Council's CCTV Scheme, 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.

II Data Protection Legislation

a. The use of data recorded through the use of Ealing Council's CCTV Scheme is required to be registered under current Data Protection legislation.

b. Ealing Council's CCTV Scheme has been registered with the office of the Data Protection Commissioner; with the Chief Executive being nominated as the data controller.

c. All data will be processed in accordance with the principles of the Data Protection Act 1998 which, in summarized 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 notified.

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 in accordance with the Act.

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.

Note:

Although most CCTV Systems were not specifically included under the terms of the 1984 Act, all Systems come within the terms of the Data Protection Act 1998. The implementation date of the new Act was 24 October 1998. Any processing, which commences after that date, needs to be fully compliant immediately with the new Act. Any processing already underway on 24 October 1998 will have to be fully compliant with the new Act by 23 October 2001.

III Request for Information (subject access)

a. 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 to the schemes data controller.

b. The principles of Sections 7 and 8 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 this code.

c. The Data Subject Access form is reproduced at Appendix E.

IV 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:

a. 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'.

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

V 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).

VI Regulation of Investigatory Powers Act, 2000

The Regulation of Investigatory Powers Act 2000 came into effect in October 2000 and introduced a statutory framework for the use of surveillance, both overt and covert, by the Police and other agencies. Section 26 of this Act defines directed 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.*

CCTV being used intrusively will be authorised other than by this section of the Act. Appropriate guidelines already exist for intrusive surveillance.

The impact for staff in CCTV monitoring centres (and Police control rooms) is that there might be cause to monitor for some time a person or premises 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 the surveillance would not require authorisation under the Act unless it were to continue for some time. "Some time" is defined as hours rather than minutes.

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

Slow time requests shall be authorised by a Superintendent or above.

If an Authority is required immediately, an Inspector may grant this. The forms in both cases must indicate the reason for the surveillance and should fall within one of the following categories:

An Authorisation is necessary on grounds falling within this sub-section 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 sub-section 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 forms. Any Authority given should be recorded appropriately for later reference. This should include the name of the authorising officer.

All Council RIPA applications to use the Council CCTV system must be made to, and authorised by, the Director of Legal and Democratic Services.

Prior to the actual use of the Council CCTV system, Council RIPA applications authorised by the Director of Legal and Democratic Services must be further verified by a 'responsible person' (namely the CCTV System Manager) thereby ensuring use of the Council CCTV system is as stipulated in the authorisation statement.

All Police RIPA applications must be authorised in accordance with the relevant police procedure and should, as a minimum, include the authorizing police officer's name, rank, signature, a brief description of the surveillance operation and all relevant dates.

Prior to the actual use of the Council CCTV system, Police RIPA applications authorised in accordance with the relevant police procedure must be further verified by a 'responsible person' (namely the CCTV System Manager) thereby ensuring use of the Council CCTV system is as stipulated in the authorisation statement.

Forms will be available at each CCTV monitoring Centre.
Examples:

1. Where a car known to belong to drug dealers is found in a car park late at night by a patrolling police officer, the officer might task CCTV to watch the vehicle for a period of time to note who goes to and from the vehicle. This would require **Inspector** Authorisation.

2. Where crime squad officers wish to have shop premises suspected of being used for dealing in stolen goods monitored from the outside over a period of days. This would require **Superintendent** Authorisation.

3. Where officers have come across a local drug dealer sitting in the town centre and wish to have a camera monitor them so as not to divulge the observation taking place. This **would not** normally require authorisation unless a prolonged observation was to ensue.

Section 4

Accountability and Public Information

I The Public

a. For reasons of security and confidentiality, access to the CCTV control and monitoring rooms 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 Scheme.

b. Cameras will not be used to look into private residential property. Privacy zones may 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 scheme.

c. A member of the public wishing to register a complaint with regard to any aspect of Ealing Council's CCTV Scheme may do so by contacting Ealing Council Offices. Any such complaint will be dealt with in accordance with existing discipline rules and regulations to which all members of Ealing Council, including the CCTV operators, are subject. An individual, who suffers damage or distress by reason of any contravention of this Code of Practice, may be entitled to compensation from the Scheme owner or operator.

II *(Scheme owner)*

a. The Public Safety CCTV Manager named at Appendix A, being the nominated representative of the scheme owners, will have unrestricted personal access to the CCTV monitoring room and will be responsible for providing regular reports of the system to his line managers.

b. Reports are reviewed by the CCTV Steering group

c. With regard to all aspects of the scheme, including this Code of Practice and the procedural manual, consultation will take place, as required, between the owners and the managers of the system, and the CCTV Steering group.

III *(System Manager)*

a. The nominated Public Safety CCTV Manager named at Appendix A will have day-to-day responsibility for the system as a whole.

b. The scheme will be reviewed by the owner (or nominated deputy)

c. The scheme manager will ensure ***" Images are being recorded for the purposes of crime prevention public safety"*** that every complaint is acknowledged, in writing, email or Telephone within seven working days. The

acknowledgement letter will include advice to the complainant as to the enquiry procedure to be undertaken.

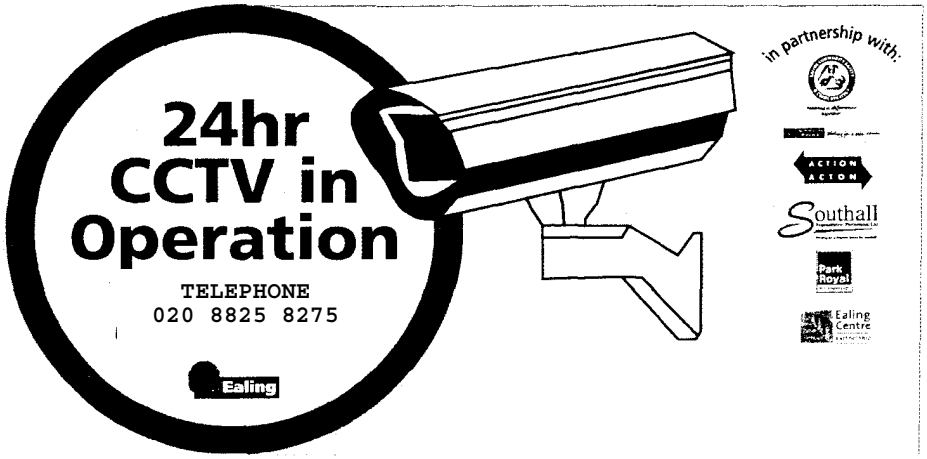
d. Statistics will be included in the yearly review with details of all complaints and the outcome of relevant enquiries. *(An informal process may be introduced whereby the system manager informs the system owner of any complaints within seven working days).*

e. Statistical and other relevant information, including any complaints made, will be included in the Review of Ealing Council's scheme and will be made publicly available on request.

IV Public Information

a. Code of Practice: A copy of this Code of Practice will be made available on request. and will be available on the Councils Website.

b. Signs: Signs will be placed on the approaches to and within the areas covered by the CCTV cameras (as illustrated below).



Section 5

Assessment of the System and Code of Practice

I Evaluation

Ealing Council's Closed Circuit Television Scheme will be periodically evaluated and audited to establish whether the purposes of the scheme are being complied with and whether objectives are being achieved. The evaluation will be incorporated in such documents as the, CCTV Strategy, as well as reports to Scrutiny ,SEP and Cabinet.

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

II Monitoring

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.

III Inspection

a. Ealing CCTV Monitoring Panel, an independent group will be responsible for inspecting the operation of the system.

b. Inspections will normally be conducted on a monthly basis with at least two *(2)* persons at any one time. It has now been agreed to allow only one monitor to attend the Control Room. The inspectors will be permitted access, without prior notice, to the CCTV control/monitoring room, 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 Auditor and their visits recorded in the CCTV control/monitoring room.

Inspectors will be required to sign a declaration of confidentiality (see Appendix (G)III Inspection

Section 6

Human Resources

I Staffing of the Control Room

a. All CCTV operators must be SIA (Security Industry Authority) trained accredited and licensed.

b. All Control Room staff will be employed directly by the Council or via the Council's appointed staffing contractor. All such staff will be required to pass stringent security appraisals to ensure their integrity before being employed as Control Room Operators. Day to day supervision of all Control Centre staff will be the responsibility of the nominated Supervisor/Manager.

c. Equipment associated with the CCTV System will only be operated by authorised personnel who will have been properly trained in its use and all control/monitoring room procedures. Each operator will be personally issued with a copy of both the Code of Practice and the Procedural Manual. They will be fully conversant with the contents of both documents, which may be updated from time to time, and which they will be expected to comply with as far as is reasonably practicable at all times.

d. Arrangement may be made for a Police liaison officer/s to be present in the monitoring room at certain times, subject to locally agreed protocols. Any such person must also be conversant with this Code of Practice.

Notes:

- *All Control Room staff will act with the upmost probity. They will not record any video image from the system other than those required by their duties, nor will they acquire, sell, borrow, copy, transmit or otherwise dispose of any images from the system.*

- *When an incident occurs, staff monitoring the CCTV system may be liable to give evidence in court, as the incident viewed on the monitor will be admissible in court as supporting evidence to the video recording itself. In these circumstances staff may be required to give a statement to a duly authorised police officer.*

II Security Screening (1)

Prior to commencing any duties in the Control Room, personnel will be subjected to full security screening (2). Personnel whose role depends upon satisfactory security screening at the commencement of employment will undergo similar screening at regular intervals, *(e.g. every 12 months)*.

Notes:

(1) The Data Protection Registrar advises that the use of enforced subject access as an ingredient of a security screening process is an abuse of data protection rights and that it is intended that such activity will eventually be criminalised. It would therefore be inappropriate to advocate such a process within this code of practice.

(2) At its meeting on 30th September 1996, the ACPO Standing Sub-Committee on the Disclosure of Convictions agreed that CCTV operatives should be vetted. (Such a vetting procedure could only be applied to those operatives working exclusively in the public domain). The process should be in line with other vetting arrangements with Local Authorities as outlined in Home Office Circular 47/93 and that indemnities should be attained. (Advice should be sought locally as police policies and procedures will vary).

It should also be noted that 'CCTV operator' is not an excepted profession under the terms of the Rehabilitation of Offenders Act 1974.

III Training and Education

a. All operators, including those who may have access to control and/or monitoring facilities at a secondary monitoring site, will be fully trained in the use of each item of equipment as well as the content of the Code of Practice and the Procedural Manual. They should also be offered training in all relevant social and legal issues (1). They will undertake continuation training on a regular basis. Operators will be encouraged to work towards formal qualification and certification of their skills and abilities with a recognised body.

b. *Others who may be involved in the use of information gathered by virtue of the CCTV System, (e.g. investigators, managers, etc.) should be properly educated in respect of the Code of Practice and the Procedural Manual. They should be made aware of the capabilities and limitations of the System and their responsibilities with regard to the handling of recorded material.*

Note:

(1) (It is recommended that initial training should be for a minimum of two days and all training should be delivered by people who are suitably qualified).

IV Discipline

a. Every individual with any responsibility under the terms of this Code of Practice and who has any involvement with the CCTV System to which they refer, will be subject to Ealing Council's disciplinary code. Any breach of this Code of Practice or of any aspect of confidentiality will be dealt with in accordance with those disciplinary rules. Any such breach may amount to gross misconduct, which could lead to dismissal. A signed undertaking to maintain confidentiality and to abide by the CCTV Code of Practice will be required of all staff.

b. The system manager will accept primary responsibility for ensuring there is no breach of security and that the Code of Practice is complied with at all times. The System Manager will be responsible for the day to day management of all aspects of the system and for enforcing the disciplinary 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.

V Welfare

Every consideration will be given to ensure the ergonomic design of the control room and monitoring stations to allow the operators to work in a safe and comfortable environment. Operators should take meal breaks away from the room and are encouraged to take short tea/coffee breaks as appropriate.

VI Health & Safety

Control Room staff will be required to have a working knowledge of the Health and Safety at Work Act 1974 (As amended) and ensure an awareness of the Health and Safety policy in respect of the Control Room, the provisions of which must be complied with at all times. Any discrepancies or concerns will be brought to the attention of the system manager who will ensure appropriate action is taken.

VII Declaration of Confidentiality

Every individual with any responsibility under the terms of this Code of Practice and who has any involvement with the CCTV Scheme to which it refers, will be required to sign a declaration of confidentiality (See example at appendix F; also Section 8 concerning access to the control/ monitoring room by others).

VIII Staffing Strategy

a. As far as is reasonably possible, authorised personnel will always be present when the CCTV monitoring and recording equipment is in use.

   Subject to the equipment functioning correctly, images from every camera will be recorded throughout every 24 hour period in time lapse mode in the Control Room Machine room only.. The DVRs will be checked to ensure that the system is fully functional at the beginning of the first shift of the day.

b. A number of the monitoring stations may not be manned on a 24 hour basis. Unmanned monitoring stations must be left secure and all operator controls switched off.

IX Further Guidance

Further guidance regarding the recruitment, selection and training of operators may be found in Police Scientific Development Branch publications: '*Recruitment and Selection of CCTV Operators' (1998, Wallace and Diffley)* and *'Training Practices for CCTV Operators' (1998, Wallace and Diffley)*.

Section *7*

Control and Operation of Cameras

I Guiding Principles

a. Any person operating the cameras will act with utmost probity at all times.

b. 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.

c. Cameras will not be used to look into private residential property. '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.

d. 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.

II Primary Control

Only those 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.

III Secondary Control

NB: Under no circumstances will the recording of information gathered from a 'public' CCTV system take place anywhere other than the designated CCTV control room.

a. Secondary *(recording),* monitoring and / or control facilities may be provided, but only when operationally necessary.

b. Subject to permission being granted by the CCTV operator, secondary control desk/s may override the control of cameras. The use of secondary control and monitoring facilities will be administered and recorded in accordance with this Code and the Procedural Manual.

c. When secondary control or monitoring of cameras is being undertaken from a location outside of the CCTV control room, the manager of that secondary site is responsible for ensuring compliance with this Code of Practice in full and at all times - especially ensuring this section is fully understood and complied with. *(Note: If secondary recording takes place, the manager of that site becomes a 'data possessor').*

IV Operation of the System by the Police

a. Under operational circumstances the Police may make a request to assume control of a camera/s from the CCTV scheme 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 schemes owners *(or designated deputy of equal standing).*

b. 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 authorised to do so and who fall within the terms of Sections 6 and 7 of this Code.

c. In very extreme circumstances a request may be made for the Police to take total control of the scheme in its entirety, including the staffing of the control room and personal control of all associated equipment to the exclusion of all representatives of the scheme owners. Any such request will only be considered personally by the most senior officer of the scheme owners (or designated deputy of equal standing). A request for total exclusive control must be made in writing by a police officer not below the rank of Assistant Chief Constable or Deputy Commissioner *(or person of equal standing).*

d. Any such operations may come under the provisions of the Regulation of Investigatory Powers Act 2000 (see Section 3).

Section 8

Access to, and Security of, Control/Monitoring Room *(and/or)* Associated Equipment

I Authorised Access

Only authorised personnel will operate any of the equipment located within the CCTV monitoring room, *(or equipment associated with the CCTV Scheme).*

II Public Access

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 visits will be conducted and recorded in accordance with the Procedural Manual.

III Equipment Demonstration

The demonstration of the capabilities and limitations of the cameras should be strictly controlled during the course of any visit with no emphasis being placed on any individual, group of individuals or property.

IV Authorised Visits

Visits by inspectors or auditors do not fall into the scope of the above paragraph and may take place at any time, without prior warning. Any such visits will be conducted and recorded in accordance with the Procedural Manual.

V Declaration of Confidentiality

Regardless of their status, all visitors to the CCTV monitoring room, including inspectors, auditors and maintenance personnel, will be required to sign the visitor's book and a declaration of confidentiality.

VI Security

Authorised personnel will normally be present at all times when the equipment is in use. If the control/monitoring facility is to be left unattended for any reason it will be secured. In the event of the control/monitoring room having to be evacuated for safety or security reasons, the provisions of the Procedural Manual (Section 4 (IX) & Section 9) will be complied with.

Section 9

Management of Recorded Material

I Guiding Principles

a. For the purposes of this Code 'recorded material' means any material recorded by, or as the result of, technical equipment which forms part of Ealing Council's Closed Circuit Television Scheme, but specifically includes images recorded digitally, or on videotape or by way of video copying, including video/ Digital prints.

b. Every video/DVR recording used in conjunction with Ealing Council's CCTV Scheme has the potential to contain material that has to be admitted in evidence at some point during its life span. Members of the community must have total confidence that information recorded about their ordinary every day activities by virtue of the scheme, will be treated with due regard to their individual right to respect for their private and family life. It is therefore of the utmost importance that every means *(e.g. video tape/CD)* of video Digital recording is treated strictly in accordance with this Code of Practice and the Procedural Manual from the moment it is delivered to the monitoring room until its final destruction. Every movement and usage will be meticulously recorded.

c. Access to, and the use of, recorded material will be strictly for the purposes defined in this Code of Practice only.

d. Recorded material will not be copied, sold, otherwise released or used for commercial purposes or for the provision of entertainment.

II National Standard for the Release of Data to a Third Party

a. Every request for the release of personal data generated by this CCTV Scheme will be channelled through the Scheme Manager *(or data controller).* The Scheme Manager will ensure the principles contained within Appendix C to this Code of Practice are followed at all times.

b. 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:

   i. Recorded material shall be processed lawfully and fairly, and used only for the purposes defined in this Code of Practice;

   ii. Access to recorded material will only take place in accordance with the standards outlined in Appendix C and this Code of Practice;

   iii. The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

c. 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.

Note:

Release to the media of recorded information, in whatever format, which may be part of a current investigation would be covered by the Police and Criminal Evidence Act 1984. Any such disclosure should only be made after due consideration of the likely impact on a criminal trial. Full details of any media coverage must be recorded and brought to the attention of both the prosecutor and the defence.

d. 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.

e. It may be beneficial to make use of 'real' footage digital or Video for the training and education of those involved in the operation of 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 scheme will only be used for such bona fide training and education purposes.

III Video Tapes Provision & Quality

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

IV Tapes Retention

a. Recorded tapes/CDs will be retained for a period of one calendar month. Before re-use or destruction, each tape will be magnetically erased.

b. Videotapes/CDs will be used in accordance with the Procedural Manual. At the conclusion of their life within the CCTV System they will be destroyed.

V Tape Register

Each tape /CD will have a unique tracking record, which will be retained for at least three years, after the tape/ CD has been destroyed.

VI Recording Policy

Subject to the equipment functioning correctly, images from every camera will be recorded throughout every 24-hour period, through digital multiplexers onto three-hour S-VHS video tapes/ DVRs. Images from selected cameras will be recorded in real time at the discretion of the CCTV operators or as directed by the System Manager.

VII Evidential Tapes

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

Section 10

Video Prints

I Guiding Principles

a. A video print is a copy of an image or images which already exist on video tape / computer disc. 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.

b. 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.

c. 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).

Appendix A

Key Personnel and Responsibilities

Neil Howard
The Public Safety CCTV Manager
Ealing Council
Parking Services
Perceval House
14/16 Uxbridge Road
London W5 2HL
Tel: 020 8825 6680

a. Responsibilities:

Ealing Council is the 'owner' of the scheme. The nominee will be the single point of reference on behalf of the owners. Their role will include a responsibility to:

i. Ensure the provision and maintenance of all equipment forming part of Ealing Council's CCTV System in accordance with contractual arrangements, which the owners may from time to time enter into.

ii. Maintain close liaison with *(the manager).*

iii. Ensure the interests of the Council and other organizations are upheld in accordance with the terms of this Code of Practice.

iv. In partnership with *(the manager),* agree to any proposed alterations and additions to the system, this Code of Practice and / or the procedural manual.

II *(Management)*

Neil Howard
The Public Safety CCTV Control Room Manager
CCTV Control Room
Old Town Hall
New Broadway
Ealing
W5 2BY

Tel: 020 8825 5104

a. Responsibilities:

i. The Public Safety Control Room Manager T is the 'manager' of the system. The nominee will be the single point of reference on behalf of the owners. Their role will include a responsibility to:

ii. Maintain day-to-day management of the system and staff;

iii. Accept overall responsibility for the system and for ensuring that this Code of Practice is complied with;

iv. Maintain direct liaison with the owners of the system.

Appendix B

Extracts from the 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, and

        ii. any information available to the data controller as the source of those data, and

    d. where the processing by automatic means of personal data of which that individual is the data subject for the 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.

10. In this section:

    ‘prescribed’ means prescribed by the Secretary of State by regulations;

    ‘the prescribed maximum’ means such amount as may be prescribed;

    ‘the prescribed period’ means forty days or such other period as may be prescribed;

    ‘the relevant day’, in relation to a request under this section, means the day on which the

data controller receives 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).

11. 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;

    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.

    Note:

    These extracts are for guidance only. To ensure compliance with the legislation, the relevant Data Protection legislation should be referred to in its entirety.

Appendix C

National Standard for the Release of Data to Third Parties

I 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 Standards Committee of *The CCTV User Group* 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 following guidance has been adopted as a nationally recommended standard by the Standards Committee of The CCTV User Group and the Local Government Information Unit in consultation with CMG Consultancy.

II General Policy

a. It is strongly recommended that local procedures should be put in place to ensure a standard approach to all requests for the release of data. It is recommended that every request is channelled through the data controller **(1)**.

Notes:

(1) *The **data controller** is the person who (either alone or jointly or in common with other persons) determines the purpose for which and the manner in which any personal data are, or are to be, processed. (In most cases the data controller is likely to be the scheme owner or manager).*

III 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 should be 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)**

vi. 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 scheme owner (or representative) should:

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, (it may be appropriate to impose a time limit on such retention which should be notified at the time of the request).

d. In circumstances outlined at note (3) below, (requests by plaintiffs, accused persons or defendants) the owner, (or nominated representative) should:

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 may not be restricted to the civil police but could include, (for example) British Transport Police, Ministry of Defence Police, Military Police, etc. (It may be appropriate to put in place special arrangements in response to local requirements).

(2) Aside from criminal investigations, data may be of evidential value in respect of civil proceedings or tribunals. In such cases a solicitor, or authorised representative of the tribunal, should be 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.

(It may be considered appropriate to make a charge for this service. 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 scheme owner should 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.

IV 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 scheme owner should ensure that:

   i. The request does not contravene, and that compliance with the request would not breach, current relevant legislation (e.g. Data Protection, 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);

   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 should 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).

V Individual Subject Access under Data Protection Legislation

a. Under the terms of Data Protection legislation, individual access to personal data, of which that individual is the data subject, must be permitted providing:

i. The request is made in writing;

ii. A specified fee is paid for each individual search;

iii. The Data Controller is supplied with sufficient information to satisfy him or her self as to the identity of the person making the request;

iv. The person making the request provides sufficient and accurate information about the time, date and place to enable the data controller to locate the information, which that person seeks (it is recognised that a person making a request is unlikely to know the precise time. Under those circumstances it is suggested that within one hour of accuracy would be a reasonable requirement);

v. The person making the request is only shown information relevant to that particular search and which contains personal data of her or him self only, unless all other individuals who may be identified from the same information have consented to the disclosure;

b. In the event of the scheme owner 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 owner 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 Code of Practice should list procedures for the release of personal data. Before data is viewed by a third party, the Data Controller must be satisfied that 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).

VI Process of Disclosure:

a. Verify the accuracy of the request;

b. Replay the data to the requisite 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 should be shown.

d. It must not be possible to identify any other individual from the information being shown, (any such information should be blanked-out, either by means of electronic screening or manual editing on the monitor screen (1)).

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 should be sent to an editing house for processing prior to being sent to the requestee.

Note:

(1) *The scheme owner is likely to breach Data Protection legislation if a person making a subject access request is able to identify any other individual from the information being disclosed. However a television image is two-dimensional and the majority of CCTV schemes do not have immediate access to the necessary technology to blank out or remove 'other data'. It is recommended that the advice of the Data Protection Registrar's office is sought in respect of any method which it is proposed should be adopted.*

VII Media Disclosure

a. In the event of a request from the media for access to recorded material, the procedures outlined under 'secondary request to view data' should be followed. If material is to be released the following procedures should 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 should state that the receiver must process the data in a manner prescribed by the data controller, e.g. specify identities/data that must not be revealed.

iii. It may also require that proof of 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 should be considered a contract and signed by both parties **(1)**.

Notes:

(1) *In the well publicised case of R v Brentwood Borough Council, ex parte Geoffrey Dennis Peck, (QBD November 1997), the judge concluded that by releasing the video footage, the Council had not acted unlawfully. A verbal assurance that the broadcasters would mask the identity of the individual had been obtained. Despite further attempts by the Council to ensure the identity would not be revealed, the television company did in fact broadcast footage during which the identity of Peck was not concealed. The judge concluded that tighter guidelines should be considered to avoid accidental broadcast in the future.*

VIII Principles

In developing 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 should 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 should 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 should be specifically prohibited.

Appendix D

Example of Restricted Access Notice

WARNING
ACCESS TO THIS AREA IS RESTRICTED

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 are acknowledging 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'

Appendix E

Data Subject Access

Ealing Council and The Data Protection Act

Your rights to access your own information

The Data Protection Act 1998 came into force on 1 March 2000. It sets rules for processing personal information and applies to some paper records, and to computer records.

The Data Protection Act gives you certain rights. It means organisations like Ealing Council, which may record and use personal information (for example, housing or social services records), must be open about how the information is used. They must also follow the eight principles of 'good information handling'.

The sort of data the council may have about you is information which helps the council make informed decisions about your welfare and your entitlements. This could be for awarding council tax or housing benefits, student grants or awards, social services or council housing records or your personal file if you are a council employee, for example.

Ealing is committed to the eight principles of 'good information handling'

Data must be:

1 Fairly and lawfully processed
2 processed for limited purposes
3 adequate, relevant and not excessive
4 accurate
5 not kept for longer than necessary
6 processed in line with your rights
7 secure
8 not transferred to countries outside of the European Economic Area without adequate protection.

These eight principles are legally binding.

You are entitled to find out what information, if any, Ealing Council holds about you

You are entitled to find out what information is held about you on either computer or some paper records. A list of the types of information held by each organisation known as the 'Register of Notifications' is held at the Office of the Data Protection Commissioner (see page 44).

The list Ealing has sent to the Data Protection Commissioner is available to view on the council website (www.ealing.gov.uk). From this list (called 'notification') you can see the broad types of information Ealing holds. This information does not name the people we have information about. You can access this information from your local library if you do not have your own access to the Internet.

You need to ask to see information held about you to which the Data Protection Act applies. Your request must be made in writing. This form also covers access to Housing and Social Services records.

To make this easier, we have included a form on the back page of this leaflet to use if you wish. Simply fill in and post to:

The Data Controller
ICT Services
Ealing Council
Perceval House
14/16 Uxbridge Road
Ealing
W5 2HL

You can also download a copy of the form from the Ealing Website. It is important to keep a copy of your letter or request and any further correspondence. The Data Protection Commissioner recommends sending your request by recorded delivery so you know it reaches the destination, and the date you sent it. Ealing's data controller will then contact you to ask for more details in order to confirm your identity.

You are entitled to receive the information you requested within 40 days. We are entitled to charge for providing this information. Ealing Council has decided that reasonable requests will not incur a fee.

What will be sent to me?

Ealing Council will send you a copy of any information we have about you if it is practical. There will also be a description of why your information is processed, whom it may have been passed on to or seen by outside of Ealing Council, and the logic involved in any automated decisions if requested.

Depending on the information, it may be sent to you as a computer printout, in a letter or on a form. If it is not practical to send you the information you have requested, for example it is contained in a large file, you will be given an opportunity to see the information held about you.

Can I see all the information held about me?

There are some exceptions. For example, if the information would adversely effect the detection of crime or assessing taxes or duty. Some health and social work details may also be limited.

If you think information is being kept from you and shouldn't be, contact Ealing's Data Controller on 020 8825 5000, dataprotection@ealing.gov.uk or the Data Protection Commissioner's information line 01625 545 745.

Where else can I turn to?

The Data Protection Commissioner is the 'people's champion' for data protection. If you believe one of the principles has been broken, (or any other requirement of the Data Protection Act) and you are unable to sort out the problem yourself, you can ask the Data Protection Commissioner to assess the situation.

The Commissioner is able to take enforcement action against an organisation if the matter cannot be settled informally.

You can find out more about your rights under the Data Protection Act from the Commissioner.

The Office of the Information Commissioner - Information Line: 01625 545 745, website: Www.dataprotection.gov.uk; email: mail@dataprotection.gov.uk

Or write to:

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 SAF

REQUEST FOR INFORMATION ABOUT YOU

Please answer the following questions to enable us to provide the information you require.

1. PERSONAL DETAILS

Name……

Present Address……
……
……Postcode……
Telephone number……..E-mail……
Date of birth……

If you no longer live in Ealing what was your Ealing address

Previous Address……
……
……..Post code ……

2. You have the right to see all the personal data that Ealing Council holds about you. However the Council holds a lot of data and it is difficult for us to know exactly what data is held about you and which services you have dealt with. You may wish to restrict your application to one or more specific services. Please indicate below those services for which you want access to personal data held about you. If you tick ALL please also tick all services that you think you may have dealt with.

ALL — Tick box and indicate services you may have dealt with below ☐

Housing		**Social Services**		**Education**	
● Benefits		● Adults		● Schools	
● Rents		● Children		● Youth Service	
● Repairs		● Mental Health		● Play Service	
● Allocations		● Environmental Services		● Pupil Benefits	
● Homeless Persons		● Planning		● Community Art & Museums	
● Council Tax		● Refuse Collection		● Education Social Workers	
● CCTV		● Street Cleaning		● Student Awards	
		● Building Control		● Special Education Needs	
		● Consumer Advice		● Leisure Services	
				● Library Services	

Other – specify

Please supply any further information that may assist us to find all the personal data requested. For example, names of people you have dealt with and dates when you had dealings with Ealing Council:

……
……
……

3. Data Subject declaration

In exercise of the right granted to me under the terms of the Data Protection Act 1998 I request that, you provide me with a copy of the personal data about me which you process for the purposes I have indicated in section 2. I understand that if this is not practical you will contact me and make other arrangements for me to see the information.

I confirm that I am the Data Subject and not someone acting on his/.her behalf. (The Data Controller may ask for verification of your identity). I understand that I may be liable for prosecution if I have given false information.

Signed …… Mr./Mrs./Ms/Dr. Date ……

4. Person Acting on behalf of Data Subject

I confirm that I am acting on behalf of the Data Subject and have submitted proof of my authority to do so.

Name……

Address……
……
……Post code……

Telephone Number ……E mail……

Signed…… Mr/Mrs/Ms/Dr. Date ……

Appendix F

Example of Declaration of Confidentiality

Ealing Council's CCTV Scheme

I, **(…….)** am retained by **(Ealing Council)** to perform the duty of CCTV Operator /Manager *(or other authorised role as appropriate).* I have received a copy of the Code of Practice in respect of the operation and management of that CCTV Scheme.

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 Ealing Council's CCTV Scheme, 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 Scheme, 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 Scheme).

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 the…….day of …….. Year 200…….

Appendix G

Inspector's Declaration of Confidentiality in respect of the Ealing Council's CCTV Scheme

I, **(…….)** am a voluntary inspector of Ealing Council's CCTV Scheme with a responsibility to monitor the operation of the Scheme and adherence to the Code of Practice. 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 my voluntary duties and the content of that Code of Practice. I undertake to inform the Scheme Manager *(and/or the Scheme Owner)* of any apparent contraventions of the Code of Practice that I may note during the course of my visits to the monitoring facility.

If now, or in the future I am, or I become unclear of any aspect of the operation of the Scheme 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 voluntary duties that I do not disclose or divulge to any firm, company, authority, agency, other organisation or any individual, any information which I may have acquired in the course of, or for the purposes of, my position in connection with the CCTV Scheme, verbally, in writing or by any other media, now or in the future, (including such time as I may no longer be performing the role of inspector).

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 voluntary duties, whether received verbally, in writing or any other media format - now or in the future.

Signed: …… Print Name: ……

Witness: …… Position: ……

Dated the……day of …….. Year 200…….

References

CCTV User Group — *Model Code of Practice*

Kitchin H (1996) — *A Watching Brief, A Code of Practice for CCTV.* **Local Government Information Unit**

Her Majesty's Stationery Office (1985) — *The Police and Criminal Evidence Act 1984.* **HMSO**

Her Majesty's Stationery Office (1995) — *The Police and Criminal Evidence Act 1984, Codes of Practice, April 1995.* **HMSO**

Her Majesty's Stationery Office (1996) — *The Criminal Procedures and Investigations Act 1996.* **HMSO**

The Stationery Office (1998) — *The Data Protection Act 1998.* **The Stationery Office**

The Stationery Office (1998) — *The Human Rights Act 1998.* **The Stationery Office**

The Stationery Office (2000) — *The Regulation of Investigatory Powers Act, 2000.* **The Stationery Office**