



L. B. Waltham Forest

Code of Practice

in respect of the operation of

Closed Circuit Television

Contents

Title Page	i
Contents	ii
Preface	iii
Introduction and Objectives	Section 1
Statement of Purpose and Principles	Section 2
Privacy and Data Protection	Section 3
Accountability and Public Information	Section 4
Assessment of the System and the Code of Practice	Section 5
Human Resources	Section 6
Control and Operation of the Cameras	Section 7
Access to, and Security of, Monitoring Room and / or Associated Equipment ...	Section 8
Management of Recorded Material	Section 9
Video Prints	Section 10

References

Appendices

Key Personnel and their Responsibilities	Appendix A
Extracts from the Data Protection Act, 1998	Appendix B
National Standard for the Release of Data to Third Parties	Appendix C
Restricted Access Notice	Appendix D
Declaration of Confidentiality (Operator/Manager)	Appendix E
List of Camera locations	Appendix F
Extracts from the Human Rights Act 1998	Appendix G

Preface

Since its introduction to retailers in 1967 and to a town centre in 1985, the use of closed circuit television 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 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.

The Standards Committee of *The CCTV User Group* (of which the L.B.Waltham Forest is a member), is committed to the belief that everyone has the right to respect for his or her private and family life and their home. Members of the Committee also believe that there should be no interference by any public body with the exercise of this right, except such as may be in accordance with the law, and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. In the absence of UK legislation to support these principles, and being very aware of the inherent weaknesses if effective control and monitoring procedures are not put in place, a Model Code of Practice and Procedural Manual were written and were the culmination of two years research, development and consultation by members of the Standards Committee and their Advisors.

This Code of Practice, in conjunction with the Procedural Manual, are both based on those Models and is intended as far as reasonably practicable, to safeguard the integrity of any CCTV System, whilst ensuring the right to privacy is not breached.

Code of Practice in Respect of the Operation of CCTV in the London Borough of Waltham Forest

Certificate of Agreement

The content of both this Code of Practice and the Procedural Manual are hereby approved in respect of the L.B.Waltham Forest Closed Circuit Television System and, as far as 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

Signature: Name:

Position held:

Dated the day of 20...

Signed for and on behalf of

Signature: Name:

Position held:

Dated the day of 20...

Section 1**Introduction and Objectives****I Introduction**

A Closed Circuit Television (CCTV) system has been introduced to make L.B. Waltham Forest a safe and secure environment for residents and visitors alike, and to encourage shoppers and businesses back into the borough both during the day and evening. The system, which is known as the 'The L.B. Waltham Forest CCTV System', comprises a number of cameras installed at strategic locations. The majority of the cameras are fully operational with pan, tilt and zoom facilities. (A few others are fixed cameras, images from which are presented in the same room). Secondary monitoring and control facilities are located at Chingford Police control room (but there are no recording facilities other than in the main monitoring room).

The L.B. Waltham Forest CCTV System has evolved from the formation of a community safety partnership (SafetyNet) of which the council and the Metropolitan Police are the leading partners. For the purposes of this document, the 'owner' of the system is L.B. Waltham Forest and therefore the 'data controller'⁽¹⁾. Details of key personnel, their responsibilities and contact points are shown at appendix A to this Code.

II Objectives of the System

- a) During the early stages of negotiation the partnership stated the objectives of the CCTV System as being;
- To help reduce the fear of crime,
 - To help deter crime and detect crime
 - To enhance community safety, boost the economy and encourage greater use of the town centre / shopping areas, etc.
 - To assist the Local Authority in its enforcement and regulatory functions within the borough
 - To assist with traffic management
 - To assist in supporting civil proceedings help detect crime.
 - To discourage anti-social behaviour, including alcohol and drug related issues.

III Procedural Manual

This Code of Practice (hereafter referred to as 'the Code') will be supplemented by a separate procedural manual, which offers 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.

Note

- (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).

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 the L.B. Waltham Forest CCTV System, (hereafter referred to as 'The System') and to outline how it is intended to do so.

II General Principles

- a) The System 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 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, and will conform with the Data Protection and Human Rights Acts.
- 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 System 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 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.

III Copyright

Copyright and ownership of all material recorded by virtue of the L.B. Waltham Forest CCTV System will remain with the data controller

IV Cameras and Area Coverage

The areas covered by CCTV to which this Code of Practice refers are spread throughout the borough, the updated list is in Appendix G to this document. The majority of the cameras offer full colour, pan tilt and zoom (PTZ) capability, some of which can be switched in low light conditions, to provide an enhanced picture for better quality. None of the cameras are installed in a covert manner.

V Monitoring and Recording Facilities

- a) A fully staffed monitoring room is located within the Walthamstow town hall complex. The CCTV equipment has the capability of recording all cameras simultaneously throughout every 24 hour period.
- b) CCTV operators are able to record images from selected cameras in real time, produce copies of recorded images, replay or copy any pre-recorded data at their discretion and in accordance with the Code of Practice, Data Protection and Human Rights Acts.

VI Human Resources

Authorised persons will normally 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⁽¹⁾ and handled strictly in accordance with this Code of Practice and the Procedural Manual.

VIII Operators Instructions

Instructions on the use of equipment housed within the monitoring room are contained in a separate manual provided by the equipment suppliers and also in the Procedural Manual.

IX Changes to the Code or the Procedural Manual

- a) Any major changes to either the Code 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, and upon the agreement of all organisations with a participatory role in the operation of the system.
- 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) 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) organisation, 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) 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.

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) organisation, adaptation or alteration of the information or data;
 - ii) retrieval, consultation or use of the information or data;
 - iii) disclosure of the information or data by transmission, dissemination or otherwise making available, or
 - iv) alignment, combination, blocking, erasure or destruction of the information or data.
- b) All personal data obtained by virtue of the L.B. Waltham Forest CCTV System, shall be processed fairly and lawfully and, in particular, shall only be processed in the exercise of achieving the stated objectives of the system. In processing personal data there will be total respect for everyone's right to respect for his or her private and family life and their home.

II Data Protection Legislation

- a) Although the System at present is not required to be registered, 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.

[Although most CCTV Systems were not specifically included under the terms of the 1984 Act, most, if not all Systems will 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 system manager, (or data controller).
- b) The principles of Sections 7 and 8 of the Data Protection Act 1998 (Rights of Data Subjects and Others) should be followed in respect of every request, those Sections are reproduced as appendix B to these codes.

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).

Section 4

Accountability and Public Information

I The Public

- a) 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, or nominated representative. Any such visits will be conducted and recorded in accordance with the Procedural Manual.
- 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 interior of any private residential property within range of the system is not surveyed by the cameras.
- c) A member of the public wishing to register a complaint with regard to any aspect of the L.B. Waltham Forest CCTV System may do so by contacting the Chief Executives office. Any such complaint will be dealt with in accordance with existing discipline rules and regulations to which all members of the council, including the CCTV operators, are subject.

II (System owner)

- a) The L.B. Waltham is the "owner" of the system, however the Executive Director of Corporate Services, is the nominated representative of the system owners and will have unrestricted personal access to the CCTV monitoring room and will be responsible for receiving regular and frequent reports from the manager of the system.
- b) The Chief Executives Office may nominate a committee with a specific responsibility for receiving and considering those reports.
- c) Formal consultation will take place between the owners and the managers of the system with regard to all aspects, including this Code of Practice and the procedural manual.

III (System manager)

- a) The nominated manager named at appendix A will have day-to-day responsibility for the system as a whole.
- b) The system will be audited by Consultants, (or nominated deputy whose organisational level of responsibility is at least equal to that of the system manager, but not the system manager).
- b) The system manager will ensure that every complaint is acknowledged in writing within five working days which will include advice to the complainant of the enquiry procedure to be undertaken. A formal six monthly report will be forwarded to the nominee of the system owner named at appendix A, giving details of all complaints and the outcome of relevant enquiries.

- c) Statistical and other relevant information, including any complaints made, will be included in the Annual Report of Corporate Services, Emergency Response & Planning and will be made publicly available.

IV. Public Information

- a) Code of Practice: A copy of this Code of Practice, will be made available to anyone requesting them. Additional copies will be lodged at public libraries, Chingford and Leyton Metropolitan Police stations and relevant offices of L.B. Waltham Forest Local Authority..
- b) Annual Report: A copy of the annual report will also be made available to anyone requesting it. Additional copies will be lodged at public libraries, Chingford and Leyton Metropolitan Police stations and offices of L.B. Waltham Forest Local Authority.
- d) Signs: Signs will be placed in the locality of the cameras and at main entrance points to the relevant areas, e.g. Railway and Bus stations. The signs will indicate:
 - i) The presence of CCTV monitoring,
 - ii) The 'ownership' of the system, i.e. the partners involved.

Note:

It is recommended that the nationally recognised sign developed by The CCTV User Group should be adopted. The design and wording of the sign has been approved by the Standards Committee of the CCTV User Group and The Department of Transport (Advertising Section). The sign has also been assessed by the office of the Data Protection Commissioner and the Police Scientific Development Branch of the Home Office.

Section 5

Assessment of the System and Code of Practice

I) Evaluation

II)

The L.B. Waltham Forest Closed Circuit Television System will periodically be independently evaluated to establish whether the purposes of the system are being complied with and whether objectives are being achieved. The evaluation will incorporate such things as (*for example, but not limited to*):

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

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

(It is recommended that evaluations should take place at least every two years)

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) Audit

The Chief Executive's Office, or a nominated officer, 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, video tape histories and the content of recorded material.

IV) Inspection

- a) A body of individuals who have no direct contact with the system will be responsible for inspecting the operation of the system.
- b) Inspections should take place periodically by no more than (*two*) people at any one time. The inspectors will be permitted access to the CCTV monitoring room, without 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 Auditor and their visit recorded in the CCTV monitoring room.

Human Resources

I Staffing of the Monitoring Room

- a) The CCTV Monitoring Room will be staffed in accordance with the procedural manual. Equipment associated with the CCTV System will only be operated by authorised personnel who will have been properly trained in its use and all monitoring room procedures. Each operator will be personally issued with a copy of both the codes 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 he / she will be expected to comply with as far as is reasonably practicable at all times.
- b) 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 these Codes of Practice and associated Procedural Manual.

II 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 the Council's 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.
- 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. 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.

III Declaration of Confidentiality

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 required to sign a declaration of confidentiality. (See example at appendix E, see also Section 8 concerning access to the monitoring room by others).

Section 7**Control and Operation of Cameras****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 and the Procedural Manual.
- 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 (*where applicable*)

NB: It is highly recommended that under no circumstances will the recording of information gathered from a 'public' CCTV system take place anywhere other than the designated CCTV monitoring room.

- a) Secondary monitoring and / or control facilities may be provided at Chingford Police station control room.
- b) Subject to permission being granted by the CCTV operator, secondary control desks may take control of cameras, however the main control room has over-riding control at all times. 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 monitoring 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.

IV Operation of the System by the Police

- a) Under extreme circumstances the Police may make a request to assume control of the CCTV System to which this Code of Practice applies. Only requests made on the authority of a police officer not below the rank of Inspector (or designated representative) will be considered. Any such request will only be accommodated on the personal authority of the most senior representative of the System owners, *(or designated deputy of equal standing)*.
- b) In the event of such a request being permitted, the Monitoring Room will continue to be staffed, and equipment operated by, only those personnel who are authorised to do so and who fall within the terms of Sections six and seven of this Code.
- c) 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 will only be considered personally by the most senior officer of the System 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 of Deputy Commissioner *(or person of equal standing)*.

V Use of the system

- a) In certain circumstances the Police or other council departmental officers may request the partial use of the CCTV system to carry out specific tasks. (i.e. fly tipping, parking violations, bus lane infringements, or a covert operation to target criminals.)

All requests must be agreed by the systems manager or representative and all procedures adhered to.

- b) Depending on the nature of the request and duration the requesting officer may be permitted to use the systems second keyboard. All secondary use of the system must be entered into the Daily log.
- c) Priority at all times must be given to the CCTV operator.

Section 8**Access to, and Security of, 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 System)*.

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 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. 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.

IV Declaration of Confidentiality

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

Note It is recommended that each page of the visitors book contains a declaration containing wording similar to: 'In signing this visitor's book all visitors to the CCTV monitoring room acknowledge that the precise location of the CCTV monitoring room is, and should remain, confidential and that they agree not to divulge any information obtained, overheard or overseen during their visit'. Consideration may also be given to displaying a notice at the entrance to the room and to including reference to that notice in the declaration by visitors. An example of an appropriate notice is attached at appendix D).

V Security

Authorised personnel will normally be present at all times when the equipment is in use. If the monitoring facility is to be left unattended for any reason it will be secured. In the event of the monitoring room having to be evacuated for safety or security reasons, the provisions of the Procedural Manual 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 the L.B. Waltham Forest Closed Circuit Television System, but specifically includes images recorded digitally, or on videotape or by way of video copying, including video prints.*
- b) Every video recording used in conjunction with the L.B. Waltham Forest CCTV System has the potential of containing material that has to be admitted in evidence at some point during its life span.
- c) Members of the community must have total confidence that information recorded about their ordinary every day activities by virtue of the system, will be treated with due regard to their individual right to respect for their private and family life.
- d) It is therefore of the utmost importance that every means (*e.g. video tape*) of video 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.
- e) Access to, and the use of, recorded material will be strictly for the purposes defined in this Code of Practice only.
- f) 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 System will be channelled through the System Manager (*or data controller*). The System 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' 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.

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 video tapes 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 will be retained for a period of 28 days. Before reuse or destruction, each tape will be magnetically erased.
- b) Videotapes 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 will have a unique tracking record, which will be retained for at least three years, after the tape has been destroyed.

VI Recording Policy

Subject to the equipment functioning correctly, images from every camera will be recorded throughout every 24 hour period in 24 hour time lapse mode, through digital multiplexers onto three hour S-VHS video tapes. 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 being required for evidential purposes the procedures outlined in the Procedural Manual will be strictly complied with.

Appendix A

Key Personnel and Responsibilities

(I) **(Ownership)**

L.B. Waltham Forest
Chief Executives office
Tel: 0208-496-3000

a) Responsibilities:

L.B. Waltham Forest is the 'owner' of the system, and therefore the "data controller". The nominee, the Executive Director of Corporate Services will be the single point of reference on behalf of the owners. His / Her role will include a responsibility to.

- i) Ensure the provision and maintenance of all equipment forming part of the L.B. Waltham Forest CCTV System in accordance with contractual arrangements that the owners may from time to time enter into.
- ii) Maintain close liaison with the System Manager.
- iii) Ensure the interests of L.B. Waltham Forest and other organisations are upheld in accordance with the terms of this Code of Practice.
- iv) *In partnership with the Systems Manager, agree to any proposed alterations and additions to the system, this Code of Practice and / or the Procedural manual.*

II **(Management)**

Corporate Services Directorate
Emergency Response
Tel: 0208 -523-1528

a) Responsibilities:

The Executive Director of Corporate Services is the 'manager' of the system. The nominee, the Systems Operations Manager, Emergency Response, will be the single point of reference on behalf of the managers. His / Her role will include a responsibility to.

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

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 peoples 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.

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).
- Note:** a time limit could apply providing reasonable notice was issued to the agent, prior to the destruction of the held data, (e.g. a time limit was about to expire).
- d) In circumstances outlined at note (3) below, (requests by plaintiffs, accused persons or defendants) the 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.

A 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 in ½ hour segments)

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 data controller should be satisfied that the data is:
 - i) Not currently and, as far as can be reasonably ascertained, not likely to become, part of a 'live' criminal investigation;
 - ii) Not currently and, as far as can be reasonably ascertained, not likely to become, relevant to civil proceedings;
 - iii) Not the subject of a complaint or dispute which has not been actioned;
 - iv) The original data and that the audit trail has been maintained;
 - v) Not removed or copied without proper authority;
 - vi) For individual disclosure only (i.e. to be disclosed to a named subject)

VI 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 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

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' 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

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.

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'

Example of Declaration of Confidentiality

The L.B. Waltham Forest CCTV System

I, am retained by L.B. Waltham Forest to perform the duty of CCTV operator. I have received a copy of the Code of Practice in respect of the operation and management of that CCTV System.

I hereby declare that:

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

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

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

Signed: Print Name:

Witness: Position:

Dated the day of

Extracts from the Humans Rights Act 1998

THE CONVENTION GUARANTEES THE FOLLOWING RIGHTS AND FREEDOMS

- Article 2. The right to life.
- Article 3. Freedom from torture or inhuman or degrading treatment.
- Article 4. Freedom from slavery.
- Article 5. The right to liberty and security of the person.
- Article 6. The right to a fair and public trial within a reasonable time.
- Article 7. The right to freedom from retrospective criminal law and no punishment without law.
- Article 8. The right to respect for private and family life, home and correspondence.
- Article 9. The right to freedom of thought, conscience and religion.
- Article 10. The right to freedom of expression.
- Article 11. The right to freedom of assembly and association.
- Article 12. The right to marry and found a family.
- Article 14. The prohibition of discrimination in the enjoyment of convention rights.

Protocol 1 to the convention has added:

- Article 1. The right to peaceful enjoyment of possessions and protection of property.
- Article 2. The right to access to education.
- Article 3. The right to free elections.