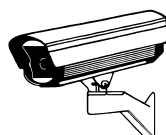


**The County of
Herefordshire District Council**

in partnership with

West Mercia Police



Code of Practice for the Operation of Closed Circuit Television

OCTOBER 2011

Safer
Herefordshire

The County of Herefordshire District Council
Brockington, 35 Hafod Road, Hereford. HR1 1SH
Tel: 01432 260000 Fax: 01432 260286

www.herefordshire.gov.uk

Contents

Certificate of Agreement

Record of Approved Changes to The Code

SECTIONS		PAGE
Section 1	Introduction and Objectives	5
Section 2	Statement of Purpose and Principles	7
Section 3	Privacy and Data Protection	9
Section 4	Accountability and Public Information	11
Section 5	Assessment of The System and The Code	13
Section 6	Human Resources	14
Section 7	Control and Operation of Cameras	15
Section 8	Access to and Security of The Control Room and Associated Equipment	17
Section 9	Management of Recorded Material	18
Section 10	Video Prints	20
 SCHEDULES		
Schedule 1	Locations of Cameras	21
Schedule 2	Key Personnel and Responsibilities	22
Schedule 3	Operational Procedures	23
Schedule 4	Complaints Procedure	30
Schedule 5	Extracts from Data Protection Act 1998 and Data Protection Code of Practice July 2000	32
 APPENDICES		
Appendix A	National Standard for the Release of Data to Third Parties	60
Appendix B	Restricted Access Notice Warning	64
Appendix C	Declaration of Confidentiality	65
Appendix D	Inspector's Declaration of Confidentiality	66
Appendix E	Subject Access Request Form	67
Appendix F	Maps of Herefordshire Camera Locations	72
Appendix G	Regulation of Investigatory Powers Act 2000 (RIPA) Guiding Principles	73
Appendix H	Glossary	77

CODE OF PRACTICE FOR THE OPERATION OF CCTV IN HEREFORDSHIRE

Agreed by

**The County of Herefordshire District Council
In consultation and partnership with
West Mercia Police**

Certificate of Agreement

The content of both The Code and the Operational Procedures are hereby approved in respect of The System and, as far as is reasonably practicable, will be complied with all who are involved in the management and operation of The System.

Signed for and on behalf of The County of Herefordshire District Council



Signature:

Name: Geoff Hughes Position held: Director of Places and Communities

Dated the 1st day of October 2011

RECORD OF APPROVED CHANGES TO THE CODE

Date	Reference	Comment	By
Jul 2005	Version 1.0		DJS
August 2009	Version 2.0	Updated change of name for Partnership and West Mercia Police, new camera locations and address for SARs.	DJS
October 2011	Version 3.0	Updated Job Title, new camera locations	DJS

Section 1 Introduction and Objectives

1.1 Introduction

Closed Circuit Television (CCTV) systems have been installed at the locations specified in Schedule 1 attached. These systems, collectively known as The System, comprise a number of cameras installed at strategic locations. All of the cameras are fully operational with pan, tilt and zoom facilities, except for Church Lane, Ledbury, which is a static camera. Primary monitoring, recording and control facilities are located in Hereford. Images can be viewed only at Hereford Police Station (The Police Station).

The System has evolved from the formation of a partnership between The County of Herefordshire District Council and West Mercia Police (The Partnership) who in consultation have agreed their acceptance of the requirements of this Code of Practice (The Code).

For the purposes of this document, the 'owner' of The System is The County of Herefordshire District Council (The Herefordshire Council).

For the purposes of the Data Protection Act the Data Controller is The County of Herefordshire District Council. The Data Controller is the person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are to be processed. It must be a legal entity e.g. person, organisation or corporate body and in the case of partnerships all partners may be considered to bear the responsibility.

The System Manager is The Herefordshire Council.

The System has been notified to the Information Commissioner.

Details of key personnel, their responsibilities and contact points are shown in Schedule 2 to The Code.

1.2 Partnership Statement in Respect of The Human Rights Act 1998

1.2.1 The Partnership recognises that public authorities and those organisations carrying out the functions of a public service nature are required to observe the obligations imposed by the Human Rights Act 1998, and consider that the use of CCTV in Herefordshire is a necessary, proportionate and suitable tool to help reduce crime, reduce the fear of crime and improve community safety.

1.2.2 This assessment is evidenced by an agreed 'operational requirement' document. Section 163 of the Criminal Justice and Public Order Act 1994 creates the power for local authorities to provide CCTV coverage of any land within their area for the purposes of crime prevention or victim welfare and it is also considered a necessary initiative by The Herefordshire Council and West Mercia Police towards their duties under the Crime and Disorder Act 1998.

1.2.3 It is recognised that the operation of The System may be considered to infringe on the privacy of individuals. The Partnership recognises that it is its responsibility to ensure that The System should always comply with all relevant legislation, to ensure its legality and legitimacy. The System will only be used as a proportional response to identified problems and be used only in so far as it is necessary in a democratic society, in the interests of national security, public safety, the economic well being of the area, for the prevention and detection of crime or disorder, for the protection of health and morals, or for the protection of the rights and freedoms of others.

1.2.4 The Code and observance of the Operational Procedures as Schedule 3 attached shall ensure that evidence is secured, retained and made available as required to ensure that there is absolute respect for everyone's right to a fair trial.

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

1.3 Objectives of The System

1.3.1 The objectives of The System as determined by The Partnership which form the lawful basis for the processing of data are to: -

- help reduce the fear of crime
- help deter crime
- help detect crime and provide evidential material for court proceedings
- assist in the overall management of the town centres of Hereford, Ledbury, Leominster and Ross-on-Wye
- enhance community safety, assist in developing the economic well being of Herefordshire and encourage greater use of the town centres, shopping centres, car parks, etc.
- assist The Partnership in its enforcement and regulatory functions within Herefordshire
- assist in traffic management

1.3.2 Within this broad outline, The Partnership, have drawn up and published the key objectives (which will be reviewed annually) based on local concerns as detailed in Paragraph 1.3.1 above.

1.4 Operational Procedures

The Code is supplemented by the Operational Procedures that offer instructions on all aspects of the day-to-day operation of The System. To ensure that the purpose and principles, see Section 2, of The System are realised, the Operational Procedures are based and expand upon the contents of The Code.

Section 2 Statement of Purpose and Principles

2.1 Purpose

- 2.1.1 The purpose of this document is to state the intention of the owners and the managers as listed in Schedule 2, on behalf of The Partnership as a whole and as far as is reasonably practicable, to support the objectives of The System, and to outline how it is intended to do so.
- 2.1.2 The purpose of The System, and the process in determining the reasons for implementing The System is as previously defined in order to achieve the key objectives detailed within Section 1 above.

2.2 General Principles of Operation

- 2.2.1 The System will be operated in accordance with all of the requirements and the principles of the Human Rights Act 1998.
- 2.2.2 The operation of The System will also recognise the need for formal authorisation of any covert 'directed' surveillance or crime-trend ('hotspot') surveillance as required by the Regulation of Investigatory Powers Act 2000 (RIPA) and West Mercia Police policy.
- 2.2.3 The System will be operated in accordance with the Data Protection Act 1998 at all times.
- 2.2.4 The System will be operated fairly, within the law, and only for the objectives for which it was established. These purposes are identified as 1.3 The Code.
- 2.2.5 The System will be operated with due regard to the principle that everyone has the right to respect for his or her private and family life and their home.
- 2.2.6 The public interest in the operation of The System will be recognised by ensuring the security and integrity of Operational Procedures.
- 2.2.7 Throughout The Code it is intended, as far as is reasonably possible, to balance the objectives of The System with the need to safeguard the individuals' rights. Every effort has been made throughout The Code to indicate that a formal structure has been put in place, including a complaints procedure, Schedule 4 attached, by which it can be identified that The System is not only accountable, but is seen to be accountable.
- 2.2.8 Participation in The System by any organisation, individual or authority assumes an agreement by all such participants to comply fully with The Code and to be accountable under it.

2.3 Copyright

- 2.3.1 Copyright and ownership of all material recorded by virtue of The System will remain with the Data Controller.

2.4 Cameras and Area Coverage

- 2.4.1 The areas covered by The System to which The Code refers are the public areas within the responsibility of the operating partners and cover Hereford, Ledbury, Leominster and Ross-on-Wye. Detailed locations are set out in Schedule 1 attached.
- 2.4.2 None of the cameras forming part of The System are installed in a covert manner. Some cameras may be enclosed within 'All-weather domes' for aesthetic or operational reasons, but appropriate signs identify the presence of all cameras.

2.5 Monitoring and Recording Facilities

- 2.5.1 A staffed Control Room is located in Hereford. The CCTV equipment records all cameras simultaneously throughout every 24 hour period.
- 2.5.2 Viewing equipment is located at The Police Station.
- 2.5.3 CCTV Operators are able to record images from selected cameras in real-time, produce hard and WORM (Write Once Read Many) copies of recorded images, replay or copy any pre-recorded data at their discretion and in accordance with The Code. All viewing and recording equipment shall only be operated by trained and authorised users.

2.6 Human Resources

- 2.6.1 Unauthorised persons will not have access to the Control Room without an authorised member of staff being present.
- 2.6.2 Only specially selected and trained Operators in accordance with the strategy contained within the Operational Procedures shall staff the Control Room.
- 2.6.3 All Operators shall receive training relevant to their role regarding the Human Rights Act 1998, Data Protection Act 1998, Regulation of Investigatory Powers Act 2000 and The Code and Operational Procedures. Further training will be provided as necessary.

2.7 Processing and Handling of Recorded Material

- 2.7.1 All recorded material, in whatever form, will be processed and handled by all partners strictly in accordance with The Code and the Operational Procedures.

2.8 Operators' Instructions

- 2.8.1 Technical instructions on the use of equipment housed within the Control Room are contained in a separate manual provided by the equipment suppliers within the Control Room.

2.9 Changes to The Code or the Operational Procedures

- 2.9.1 Any major changes to either The Code or the Operational Procedures (i.e. such as will have a significant impact upon The Code or upon the operation of The System) will take place only upon agreement being reached between The Partners.

Section 3 Privacy and Data Protection

3.1 Public Concern

- 3.1.1 All personal data obtained by virtue of The System shall be processed fairly and lawfully and, in particular, shall only be processed in the exercise of achieving the stated objectives of The System.
- 3.1.2 The data will be securely stored strictly in accordance with the requirements of the Data Protection Act 1998 and any additional locally agreed procedures.

3.2 Data Protection Legislation

- 3.2.1 The operation of The System has been notified to the Office of the Information Commissioner in accordance with current Data Protection legislation.
- 3.2.2 The Data Controller for The System is The Herefordshire Council and day-to-day responsibility for the data will be devolved to the Commissioning Officer (CCTV).
- 3.2.3 All data will be processed in accordance with the principles of the Data Protection Act, 1998. These principles include:-
- 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 The Code.
 - iv) Only personal data will be held which is adequate, relevant and not excessive in relation to the purpose for which the data is held.
 - v) Steps will be taken to ensure that personal data is accurate and, where necessary, kept up-to-date.
 - vi) Personal data will be held for no longer than is necessary.
 - vii) Where appropriate, individuals will be allowed access to information held about them.
 - viii) Procedures will be implemented to prevent unauthorised access to, or alteration, disclosure, loss or destruction of information.

3.3 Request for Information

- 3.3.1 Any request from an individual for the access to personal data that he/she believes is recorded by virtue of The System will be directed in the first instance to the Commissioning Officer (CCTV).
- 3.3.2 The principles of Sections 7 and 8, 10 and 12 of the Data Protection Act 1998 (Rights of Data Subjects and Others) shall be followed in respect of every request. Those Sections are reproduced as Schedule 5 of The Code.
- 3.3.3 If the request cannot be complied with without identifying another individual, permission from all such other parties must be considered (in the context of the degree of privacy they could reasonably anticipate from being in that location at that time) in accordance with the requirements of the legislation.

3.3.4 Any person making a request must be able to satisfactorily prove their identity and provide sufficient information to enable the data to be located. The appropriate 'Subject Access' request form is included in Appendix E.

3.4 Exemptions to the Provision of Information

3.4.1 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 the following statement:

Personal data processed for the following purposes namely:–

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

is 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'.

Section 4 Accountability and Public Information

4.1 The Public

- 4.1.1 For reasons of security and confidentiality, access to the Control Room is restricted in accordance with The Code. 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 Commissioning Officer (CCTV).
- 4.1.2 Cameras will not be used to look into private residential property. The Operators will be specifically trained in privacy issues.
- 4.1.3 A member of the public wishing to register a complaint with regard to any aspect of The System may do so by contacting the Commissioning Officer (CCTV). All complaints shall be dealt with in accordance with The Herefordshire Council's complaints procedure, Schedule 4 attached.

Any operating staff performance issues identified will be considered under the disciplinary procedures of the staffing contractor.

- 4.1.4 All CCTV staff are contractually subject to regulations governing confidentiality and discipline. Any individual who suffers damage or distress by reason of any contravention of The Code may be entitled to compensation.

4.2 System Manager

- 4.2.1 The Commissioning Officer (CCTV) referred to in Schedule 2 will have day-to-day responsibility for The System as a whole.
- 4.2.2 The System will be subject to annual audit by the Council's audit body.
- 4.2.3 The Commissioning Officer (CCTV) will ensure that every complaint is acknowledged in writing within two working days and investigated within 8 working days. If the results of the investigation are unsatisfactory, the complainant has the right to make a formal complaint using the Council's Complaints Procedure Schedule 4 attached. A formal report will be forwarded to the nominee of The System owner named at Schedule 2, giving details of all complaints and the outcome of relevant enquiries.
- 4.2.4 Statistical and other relevant information, including any complaints made, will be included in the Annual Reports of The Council that are made publicly available.

4.3 Public Information

4.3.1 The Code

A copy of The Code will be made available to anyone on request for a nominal fee. Full copies will be lodged at all "Info in Herefordshire" Offices throughout the County.

4.3.2 Annual Report

The Annual Report for CCTV will be published and will be made available to anyone requesting it. Additional copies will be lodged at all "Info in Herefordshire" Offices throughout the County.

4.3.3 Signs

Signs (as shown below) are placed in the locality of the cameras and at the main entrance points to the relevant areas, e.g. railway and bus stations. The signs indicate:

- i) The presence of CCTV monitoring;
- ii) The 'ownership' of The System;
- iii) The contact telephone number of the 'Data Controller' of The System.



Section 5 Assessment of The System and The Code

5.1 Evaluation

5.1.1 The System will periodically be independently evaluated to establish whether the purposes of The System are being complied with and whether its objectives are being achieved. The format of the evaluation shall comply with that laid down by the Home Office Statistics and Research Directorate in the Home Office Bidding Guidelines and be based on assessment of the inputs, the outputs, the process and the impact of The System.

- i) An assessment of the impact upon crime: This assessment shall include not only the immediate area covered by the cameras but the wider town area, the Police Divisional and regional areas and national trends
- ii) An assessment of the incidents monitored by The System
- iii) The views and opinions of the public
- iv) Whether the purposes for which The System was established are still relevant

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

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

5.2 Monitoring

5.2.1 The Commissioning Officer (CCTV) has day-to-day responsibility for the monitoring, operation and evaluation of The System and the implementation of The Code.

5.2.2 The Commissioning Officer (CCTV) shall also be responsible for maintaining full management information regarding the incidents dealt with by the Control Room, for use in the management of The System and in future evaluations.

5.3 Inspection

5.3.1 A body of individuals who have no direct contact or relationship with the operation of The System will be appointed to be responsible for inspecting the operation of The System.

5.3.2 Inspections should take place at least six times per calendar year by no more than two people at any one time. The Inspectors will be permitted access to the Control 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 written findings will be reported and retained by the Council's Commissioning Officer (CCTV). The visits will be recorded in the Visitor Book held in the Control Room.

5.3.3 Inspectors will be required to sign a Declaration of Confidentiality (see Appendix D).

Section 6 Human Resources

6.1 Staffing and Management of The System

6.1.1 Every person involved in the management and operation of The System will be personally issued with a copy of The Code and the Operational Procedures, and will be required to sign a confirmation that they fully understand the obligations adherence to these documents place upon them and that any breach will be considered a disciplinary offence. 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.

6.2 Discipline

6.2.1 Every individual employed by or through The Partnership with any responsibility under the terms of The Code and who has any involvement with The System to which they refer, will be subject to their own organisation's discipline code. Any breach of The Code or of any aspect of confidentiality will be dealt with in accordance with those discipline rules.

6.2.2 The Commissioning Officer (CCTV) has primary responsibility for ensuring that there is no breach of security and that The Code is complied with. Non-compliance with The Code by any person will be considered a breach of discipline and dealt with accordingly.

6.3 Declaration of Confidentiality

Every individual with any responsibility under the terms of The Code and who has any involvement with The System will be required to sign a Declaration of Confidentiality.

Section 7 Control and Operation of Cameras

7.1 Guiding Principles

- 7.1.1 Any person operating the cameras will act with utmost probity at all times.
- 7.1.2 The cameras, control equipment, recording and reviewing equipment shall at all times only be operated by persons who have been trained in their use and the legislative implications of their use.
- 7.1.3 Every use of the cameras will accord with the purposes and key objectives of The System and shall be in compliance with The Code.
- 7.1.4 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 Commissioning Officer (CCTV).

7.2 Primary Control

- 7.2.1 Only those trained and authorised members of staff with responsibility for using the CCTV equipment will have access to the operating controls - those Operators have primacy of control at all times.

7.3 Operational Command of The System by The Police

- 7.3.1 Under rare and extreme operational circumstances, The Police may make a request to command the use of The System to which The Code applies. These circumstances may be a major incident or event that has a significant impact on the prevention and detection of crime or public safety. Such use will provide The Police with a broad overview of events in order to command the incident.
- 7.3.2 Such requests will be viewed separately to the use of The System's cameras with regard to the requirement for an authority for specific types of surveillance under the Regulation of Investigatory Powers Act 2000. See Appendix G.
- 7.3.3 Applications made as at 7.3.1 above will be considered on the written request of a Police Officer not below the rank of Superintendent. Any such request will only be accommodated upon the personal written permission of the Commissioning Officer (CCTV). In the event of an urgent need, a verbal request of the senior officer in charge, and in any case an Officer not below the rank of Inspector, will be necessary. This should be followed as soon as practicable within 72 hours by a Superintendent's written request.
- 7.3.4 In the event of such a request being permitted, the Control Room will continue to be staffed, and equipment operated by, only those personnel who are specifically trained to do so, and who fall within the terms of Sections 6 and 7 of The Code. They will then operate under the command of the Police Officer designated in the verbal/written request, taking into account their responsibilities under The Code.
- 7.3.5 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 Control Room and personal control of all associated equipment, to the exclusion of all representatives of The System owners. Any such request should be made to the Commissioning Officer (CCTV) in the first instance, who will consult personally with 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 or person of equal standing.

7.4 Maintenance of The System

- 7.4.1 To ensure compliance with the Information Commissioners Code of Practice and that images recorded continue to be of appropriate evidential quality, The System shall be maintained under a maintenance agreement.
- 7.4.2 The maintenance agreement will make provision for regular/periodic service checks on the equipment which will include cleaning of any all-weather domes or housings, checks on the functioning of the equipment, and any minor adjustments that need to be made to the equipment settings to maintain picture quality.
- 7.4.3 The maintenance will also include regular periodic overhaul of all of the equipment and replacement of equipment that is reaching the end of its serviceable life.
- 7.4.4 The maintenance agreement will also provide for 'emergency' attendance by a specialist CCTV engineer on site to rectify any loss or severe degradation of image or camera control.
- 7.4.5 The maintenance agreement will define the maximum periods of time permitted for attendance by the engineer and for rectification of the problem depending upon the severity of the event and the operational requirements of that element of The System.
- 7.4.6 It is the responsibility of the Commissioning Officer (CCTV) to ensure that appropriate records are maintained in respect of the functioning of the cameras and the response of the maintenance organisation(s).

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

8.1 Public Access

- 8.1.1 Public access to the monitoring and recording facility will be prohibited except for lawful, proper and sufficient reasons and only then with the personal authority of the Commissioning Officer (CCTV). Any such visits will be conducted and recorded in accordance with the Operational Procedures.

8.2 Authorised Visits

- 8.2.1 Visits by Inspectors or Auditors do not fall into the scope of the above paragraph and may take place at any time, without prior warning. No more than two Inspectors or Auditors will visit at any one time. Inspectors or Auditors will not influence the operation of any part of The System during their visit. The visit will be suspended in the event of it being operationally inconvenient. Any such visit should be recorded in the same way as that described above.

8.3 Declaration of Confidentiality

- 8.3.1 Regardless of their status, all visitors to the Control Room, including Inspectors, Auditors and Police Officers, will be required to sign the Visitors' Book.

8.4 Security

- 8.4.1 Authorised personnel will normally be present at all times when the equipment is in use. If the Control Room facility is to be left unattended for any reason, it will be secured. In the event of the Control Room having to be evacuated for safety or security reasons, the provisions of the Operational Procedures will be complied with.
- 8.4.2 The Control Room will at all times be secured by appropriate secure means.

Section 9 Management of Recorded Material

9.1 Guiding Principles

- 9.1.1 For the purposes of The Code, 'recorded material' means any material recorded by, or as the result of, technical equipment which forms part of The System, but specifically includes images recorded digitally, or on videotape or by way of video copying, including video prints.
- 9.1.2 Every video or digital recording obtained by using The System has the potential of containing material that has to be admitted in evidence at some point during its lifespan.
- 9.1.3 It is therefore of the utmost importance that, irrespective of the means or format of the images obtained from The System, they are treated strictly in accordance with The Code and the Operating Procedures from the moment they are received by the Control Room until final destruction. Every movement and usage will be recorded.
- 9.1.4 Access to and the use of recorded material will be strictly for the purposes defined in The Code only.
- 9.1.5 Recorded material will not be copied, sold, otherwise released or used for commercial purposes or for the provision of entertainment.

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

- 9.2.1 Every request for the release of personal data generated by The System will be channelled through the Commissioning Officer (CCTV). The Commissioning Officer (CCTV) will ensure that the principles contained within Appendix A to The Code are followed at all times.
- 9.2.2 In complying with the national standard for the release of data to third parties, it is intended, as far as reasonably practicable, to safeguard the individual's rights to privacy and to give effect to the following principles:
- Recorded material shall be processed lawfully and fairly, and used only for the purposes defined in The Code;
 - Access to recorded material will only take place in accordance with the standards outlined in Appendix A and The Code;
 - The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.
- 9.2.3 Members of the Police Force or other agency having a statutory authority to investigate and/or prosecute offences may, subject to compliance with Appendix A, 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 Operational Procedures.
- 9.2.4 If material is to be shown to witnesses, including Police Officers, for the purpose of obtaining identification evidence, it must be shown in accordance with Appendix A and the Operational Procedures.
- 9.2.5 It may be beneficial to make use of 'real' video footage for the training and education of those involved in the operation and management of The System, and for those involved in the investigation, prevention and detection of crime. Any material recorded by virtue of The System will only be used for such bona fide training and education purposes.

9.3 Digital Images

9.3.1 The recording system is a single integrated "tape less" system. Images are recorded throughout every 24 hour period, 7 days a week and are held on the Hard Drive.

9.4 Digital Image Retention

9.4.1 Digital images are retained for a period of 31 days on the Hard Drive.

9.5 Evidential Images

9.5.1 In the event of a recording being required for evidential purposes, the procedures outlined in the Operational Procedures will be strictly complied with.

9.6 Videotapes/CD/DVD - Provision and Quality

9.6.1 To ensure the quality of the tapes, CD's and DVD's, and that recorded information will meet the criteria outlined by current Home Office guidelines, the only recording medium to be used with The System are those which have been specifically provided in accordance with the Operational Procedures.

9.7 Videotape - Register

9.7.1 Each tape will have a unique tracking record maintained in accordance with the Operational Procedures. The tracking record shall identify every use and person who has viewed or had access to the tape since the initial breaking of the seal to the destruction of the tape.

Section 10 Video Prints

10.1 Guiding Principles

- 10.1.1 A video print is a copy of an image or images that already exist on videotape/computer disc. Such prints are equally within the definitions of 'data' and recorded material.
- 10.1.2 Video prints will not be taken as a matter of routine. Each time a print is made it must be capable of justification by the originator who will be responsible for recording the full circumstances under which the print is taken in accordance with the Operational Procedures.
- 10.1.3 Video prints contain data and will therefore only be released under the terms of Appendix A to The Code, 'Release of Data to Third Parties'. If prints are released to the media (in compliance with Appendix A) in an effort to identify alleged offenders or potential witnesses, full details will be recorded in accordance with the Operational Procedures.
- 10.1.4 A record will be maintained of all video print productions in accordance with the Operational Procedures.
- 10.1.5 The records of the video prints taken will be subject to audit in common with all other records in The System.

Schedule 1 Locations of Cameras

No.	Location	Town
1	Garrick House, Widemarsh Street	Hereford
2	Marks & Spencer, High Town	Hereford
3	Sandwich Shop, Eign Gate	Hereford
4	Edinburgh Wool Shop, St. Peters Street	Hereford
5	Corner of East Street/Church Street	Hereford
6	Jewellery Shop, St. Owen Street	Hereford
7	Franklin Barnes, Commercial Road	Hereford
8	Leisure Pool Car Park, St Martins Street	Hereford
9	Orange Tree, King Street	Hereford
10	Ascaris, West Street	Hereford
11	Jeanstation, Bewell Street by entrance to Tesco	Hereford
12	Market Entrance, Blackfriars Street	Hereford
13	Penhaligan Way, Opposite Football Ground	Hereford
14	Debenham Thorpe, Broad Street/King Street	Hereford
15	Imperial Hotel, Widemarsh Street	Hereford
16	Junction Commercial Street/Maylord Street	Hereford
17	Rockfield DIY, Station Approach	Hereford
18	Blueschool Street	Hereford
19	Commercial Road	Hereford
20	Union Street	Hereford
21	Cathedral Church Street	Hereford
22	Cathedral Castle Street	Hereford
23	Cathedral School Building	Hereford
101	The Crofts, Croft Lane	Ross-on-Wye
102	Nationwide/Boots, Market Place	Ross-on-Wye
103	Natwest Bank, Gloucester Road	Ross-on-Wye
104	Gallery, Broad Street	Ross-on-Wye
105	Maltings Car Park Paypoint	Ross-on-Wye
106	Red Meadow Car Park Paypoint	Ross-on-Wye
201	Fosters Corner, West Street	Leominster
202	Etnam Street Junction	Leominster
203	Grape Vaults, Broad Street	Leominster
204	Lloyds Bank, Corn Square	Leominster
205	Etnam Street Car Park/The Grange	Leominster
206	Bus Station	Leominster
301	TIC, High Street	Ledbury
302	Above Market Place Restaurant, High Street	Ledbury
303	High Street & Worcester Road	Ledbury
304	Walled Garden, Church Street	Ledbury
305	Church Lane (Static Camera)	Ledbury

Schedule 2 Key Personnel and Responsibilities

1. System Owners

The Herefordshire Council,
Brockington,
35 Hafod Road,
Hereford.
HR1 1SH

2. System Management

Commissioning Officer (CCTV),
Safer Herefordshire,
PO Box 4,
Plough Lane,
Hereford.
HR4 0XH

Tel: 01432 261713
Fax: 01432 383031

Responsibilities:

The Commissioning Officer (CCTV) is responsible for the day-to-day operational management of The System. The Commissioning Officer (CCTV) has delegated authority for data control on behalf Data Controller. The role of the Commissioning Officer (CCTV) includes responsibility to:

- i) Maintain day-to-day management of The System and the staffing contract.
- ii) Ensure that The Code is complied with on a day-to-day basis.
- iii) Maintain direct liaison with relevant operating partners.

Schedule 3 Operational Procedures

1. Introduction

These Operational Procedures have been drawn up in conjunction with The Code which sets out minimum standards expected of all employees and authorised users managing and operating The System. The efficient and legal operation of CCTV rests with the standards contained within The Code. It should be considered as a benchmark for good practice that will ensure accountability and command employee and public confidence.

The Code will be the principal document for the resolution of any difficulties or discrepancies that may arise from the operation of The System.

The Code together with these Operational Procedures, will be subject to amendment and updates as required. It is the responsibility of all staff working on The System to ensure that at all times they adhere to the contents of these documents. These documents have been written against the legal requirements of the Human Rights Act 1998, the Data Protection Act 1998 and the Regulation of Investigatory Powers Act 2000. It is incumbent upon all staff to draw to the attention of the Data Controller any departure from the terms of The Code or its related Operational Procedures.

a. Operator Duties and Responsibilities

The very nature of CCTV is that it poses an intrusive breach of an individual's privacy. The majority of those who visit or pass by cameras will do so without an understanding of the range and capability of the cameras. The Partnership recognise the very real position of trust that those who operate The System have. In recognising the legal requirements of the Human Rights Act 1998, the Data Protection Act 1998 and the Regulation of Investigatory Powers Act 2000, The Partnership has sought to provide those who operate The System with clear guidance on their duties and responsibilities.

b. Purposes of The System

The System must not be used for any purpose other than those defined in The Code. Any failure to follow The Code will result in disciplinary action being taken against members of staff. In the context of the defined purposes of The System the cameras can be used in the detection of criminal activity as well as for the safety of people visiting and working in the area immediately covered by the camera.

c. System Integrity

The CCTV Operators should have regard for the safety and well being of those using the areas covered by the cameras. In particular the individual's right to privacy must not be unduly infringed. To this end all Operators are required to:

- sign a Declaration of Confidentiality that will remain in force throughout their period of employment;
- undergo a period of training on the operation of The System and its related procedures;
- know the contents of The Code and these Operating Procedures;
- participate in regular assessments of The System that will include monitoring, auditing and inspection of both the output of The System and the associated written documentation. These processes are set out in The Code;

- be aware at all times of the potential abuse there may be in operating The System e.g. looking into private areas such as office windows or people in their vehicles, unless such actions are justified through prior information;
- attend Court as required to support evidence that might have been gathered in the course of their duties.

d. Selection and Recruitment

- The CCTV monitoring equipment is located within the Control Room and Operators are selected and recruited specifically for the role of monitoring The System.
- Each Operator will be subject to a security vet and will be expected to demonstrate their understanding of and commitment to total confidentiality at all times.

e. Training

The training required by a CCTV Operator will include company related information as well as technical and legal information. Operators will be provided with training in The System. They will be encouraged to undertake further training to industry-recognised standards. As such the Operators must know:

- the technical operation of The System including any training given by the equipment manufacturers and installers;
- how to interpret The Code and related Operational Procedures.
- the geographical location and coverage of every camera in The System;
- the legal issues surrounding privacy and potential contravention of the Human Rights Act 1998, The Data Protection Act 1998 and the Regulation of Investigatory Powers Act 2000.

f. Discipline

- CCTV Operators will be subject to relevant discipline codes. Any breach of these Operational Procedures, The Code or confidentiality will be dealt with in accordance with those discipline regulations and staff must recognize that any such breach may amount to gross misconduct, which could lead to dismissal.
- The Partnership will accept prime responsibility for ensuring that there is no breach of security and that The Code and Operational Procedures are complied with. Those having day-to-day responsibility for the management of the Control Room will also have responsibility for enforcing the discipline regulations.

g. Welfare

All staff must know and understand their duties and commitment to Health and Safety. The Control Room staff must also understand the following information relating to staff welfare.

- Meal breaks will be taken in the rest area and Operators will be encouraged to take short tea/coffee breaks during their shift as appropriate.
- Staff monitoring The System will also take as a minimum, a 10 minute break from monitoring the screens for every one hour of monitoring.
- During periods of normal operation, staff are not expected to leave The System unmonitored unless line management has given prior authorisation.

- The Partnership recognise that there may be occasions where Operators, through their normal course of duties, may witness scenes that they might find distressing or upsetting. There is local provision made for appropriate help to be available on a confidential basis to any staff member who feels they may require this service.

h. Duties of an Operator

Duties and responsibilities within the Control Room will be co-ordinated by the Supervisor and may vary on a daily basis in order of priority as incidents occur.

i. General Duties

- Keep a keen observation of The System's cameras.
- Maintain an accurate and up to date log of events and occurrences in the Daily Occurrence Log.
- Only allow authorised personnel into the Control Room.
- Use initiative and resourcefulness to deal with any situations that may arise and utilise available staff to the best possible use.
- Carry out emergency procedures as directed in the relevant Emergency Procedures or by West Mercia Police.

j. Responsibilities

- Staff the Control Room at all times.
- Maintain a constant watch of the areas covered by The System.
- React promptly and correctly to warnings and indications given by any alarm systems installed ensuring that the action taken is logged.
- Record details of all significant occurrences in the relevant log.
- Answer all telephone calls in the correct manner and act upon them appropriately and efficiently.
- Control the entry of people to the Control Room and only allow authorised personnel entry into these areas.
- Maintain cleanliness and tidiness in the Control Room at all times.
- Use initiative and resourcefulness to deal with situations that may arise and utilise available staff to the best use possible.
- Ensure that all logs are kept up-to-date and information required is entered.
- Take charge of keys and issue them only to the authorised personnel as directed by the Commissioning Officer (CCTV).
- Ensure that correct and precise information is given to colleagues on handover.

2. Operating Procedures

a. Guiding Principles

- The Operators of the cameras and associated equipment will act with the utmost probity in the execution of their duty.

- Every use of the cameras shall accord with the purposes and key objectives of the scheme and shall comply with The Code and the Operational Procedures.
- Cameras will not be used to look into “private areas”. Operators have been specifically trained in privacy issues.
- Operators should beware of exercising prejudices that may lead to complaints of The System being used for which it is intended. The Operators may have 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.

b. Observations

Operators should be alert, but not exclusively, to the following activity:

- Individuals acting suspiciously.
- Groups of people and unaccompanied or vulnerable children (especially under 8 years old).
- A person or persons being escorted against their will.
- Suspicious packages.
- A vehicle parked/broken down in a dangerous place.
- Police and other emergency vehicles (particularly at access points).

c. Specific Actions

- If an incident occurs that is of a criminal nature, inform the Police via the appropriate communications channel.
- If emergency services (fire, ambulance or other similar organisations) are required to attend the premises then call them via the appropriate communications channel.
- For all of the above, ensure that any recordings made are in “real time” and that the situation is closely monitored to ensure that the appropriate standard of images is recorded.
- If a criminal activity is suspected or being monitored, the Operator should try to zoom the camera in to obtain an “identification” standard recording. Identification is where at least half of the subjects’ body fills the screen. After a good clear view has been obtained the Operator should zoom the camera out to get a wider shot of the action. Wherever possible the subject(s) of the recording should be kept in the centre of the picture. Other cameras should be manoeuvred to obtain a recording from a different angle.
- All incidents should be recorded in the Occurrence Log even if the Police or other resources do not attend. The Operator will indicate on the Occurrence Log the resources attending and in what numbers.
- A Record of Occurrence form is to be completed in detail to compliment the entry in the Occurrence Log.

d. Access to the Control Room

- Access to the Control Room is strictly controlled and only authorised persons are entitled to be in the Control Room. A list of those authorised to enter the Control Room is available at the site.

- Under no circumstances should anyone else be in the Control Room without authorisation from the Commissioning Officer (CCTV) or designated deputy.
- Physical proof of ID and the visitor's authorisation will be checked. Only when this is done will anyone be allowed entry into the Control Room.
- Upon entry to the Control Room it is the Operator's responsibility to ensure that all visitors sign in and when leaving sign out, recording each visitor's name, time of entry and exit and purpose of visit.

e. System Check

System Check forms are kept at the Control Room.

- At the takeover of duty, the Operator will carry out a functional test of all the cameras, checking that all of the operating functions are working correctly. The results of this test must be recorded on the System Check form provided and faxed through to the Commissioning Officer (CCTV).
- The Operator must fill in the form and describe any faults in detail.
- The Control Room Supervisor will inspect all forms on a daily basis and ensure that action is being taken to rectify the problem.
- Only copies of the System Check form can be removed from the Control Room. The original must remain at the Control Room.

f. Recording Equipment

- The System will record images digitally 24 hours per day, 7 days per week onto a Hard Disc. Images can be recorded onto CD Rom, DVD and VHS.

g. Evidence

The procedure in respect of recordings, which may contain evidence that will be required by the Police, is as follows:

- Designated Police Officers will request to view a recording based upon specific time and date parameters. Operators should ensure that all such viewing requests are done so by appointment.
- The Operator will view the recording along with the Police Officer based upon specific start and finish time and date. This viewing is recorded on an Internal Viewing Form.
- Should the material viewed be relevant to an on-going criminal investigation or specific court case, the Police Officer will request a copy of the recording. This request is logged onto the Internal Viewing Form.
- The relevant material will then be copied by the Operator onto a blank video tape or CD Rom provided by the Police.
- The recording should be clearly marked as evidence and should be released only when it has been signed for on the Evidential Tape Record and the Master Log Sheet of the Evidential Tape file is completed.
- Exactly this same procedure is followed in the event of a request from the Police Ombudsman to view any recordings from The System.

h. Provision of Services to the Media

- Under no circumstances must CCTV Operators contact or speak to the media. (Media includes local radio, television, print journalists or related staff). If The Partnership has determined that you can speak to the media you will be given the appropriate authority and all the necessary information.
- Under no circumstances must you make any approaches to the media or discuss anything that you have seen or learnt through your employment as a CCTV Operator at Herefordshire.

i. Emergency Procedures

- If the need arises to evacuate the Control Room by virtue of either a security alert or fire alarm all staff will act in accordance with local instructions. If possible, and without risking the safety of any member of staff, the room should be secured on leaving. Any operations or procedures underway at the time of the evacuation should be abandoned.
- Upon returning to the room all systems should be checked to ensure that they are in proper working order and an appropriate entry should be made in the Daily Occurrence Log.

j. Data Protection Act 1998 – Subject Access Requests

- The content of recordings made by The System is “Data”, and as such is covered by the Data Protection Act 1998. People who appear in recordings (Data Subjects) have the legal right to view any material in which they appear. However the right does not extend to some types of incidents or recordings. It is the responsibility of the Data Controller to grant access to recordings and all requests must be directed to the Data Controller in writing.
- If an Operator receives a request for access to images from anyone other than a recognised Police Officer or the Commissioning Officer (CCTV) they must not discuss with them the contents of any recording observation made by The System.
- The Data Controller may require Operators to check recordings of specific incidents, but no non-authorised individuals must be present. The form, as designated in The Code, should be completed.
- Members of the public or others requesting access must be directed to the Commissioning Officer (CCTV) or be asked to give their name, address and contact telephone number so that the Commissioning Officer (CCTV) can send them the appropriate documents.

k. Requests for Observations

- The appropriate form, as designated by The Code, should be used if a request is made of the Operator to look out for a particular incident or individual. If a known individual or group of known individuals is the subject of a request and the request comes from the “public authority” e.g. Police, local authority, Customs & Excise then the Regulation of Investigatory Powers Act 2000 may apply.
- Unless in “hot pursuit” of a suspect, which would make obtaining the necessary authority impractical, then all such observation requests must be accompanied by a written authority from an Authorising Officer. In the case of the Police, this will be an officer of the rank of Inspector or above and in the case of the Herefordshire Council this will be a recognised senior officer through the Commissioning Officer (CCTV).
- In the event of a major event taking place e.g. political demonstration, sporting event, or other event that is likely to be the source of public disorder, the Police may request that a Police Officer be present in the Control Room for the duration of the event. The Officer needs to

have written authority signed by a Chief Inspector or above, which details the duration of the event with specific start and finish times detailed on the form in order to be present in the Control Room. Approval for this will be given only after consultation with the Commissioning Officer (CCTV).

Schedule 4 Complaints Procedure

The Council will actively seek to
“ensure that all customers and users of the Council's services are aware of their right to be treated equally, with respect and dignity, and of their right to complain when they believe they have been unfairly treated.”

[Source: The Herefordshire Council Equal Opportunities Policy]

The Herefordshire Council aims to provide high quality services in line with the needs of our customers

Our staff always try to provide you with a first class service in a polite, efficient and fair way. Despite our best efforts, there may be occasions when you are unhappy with something we have done, or have not done, or about a service we provide, if so, then please tell us about it so that we can try to put it right.

We value any complaints that we receive and give you our assurance that your complaint will be thoroughly investigated.

What do we mean by a Complaint?

A complaint can be broadly defined as:

“any expression of dissatisfaction by a customer about the standard of service, actions or lack of actions by the council or its staff which has affected an individual or group.”

So

If we fail to act on the request, we do it inadequately, or if we then fail to respond within a reasonable timescale and you have to write again or ring back, that is a complaint.

How do I complain?

If the person you have been dealing with has been unable to provide a response that you consider satisfactory, or if you would like to register a formal complaint, you can either:

- Complete a complaint form, (available from Info in Herefordshire shop or telephone 01432 260500 to have one sent to you) and then return it to the FREEPOST address:
Herefordshire Council Customer Complaints,
FREEPOST,
SWC2276,
HEREFORD. HR1 2ZZ
- Call into any Info in Herefordshire shop or telephone 01432 260500 and they will help you to make a complaint
- Log on to the Herefordshire Council website at www.herefordshire.gov.uk and record your complaint online; or
- E-mail: info@herefordshire.gov.uk

If you need support with making your complaint contact the Citizens Advocacy on 01432 263757 or at: Advocacy House, 103/104 East Street, Hereford, HR1 2LW.

What will we do?

- We'll acknowledge your complaint within 2 working days, confirming the name and telephone number of the person who will be dealing with your complaint.
- We'll investigate your complaint and respond to you within a further 8 working days. If we can't meet that target, we'll write and give you a progress report giving you a further date when you can expect a full response.

Still not satisfied?

With the reply to your complaint, you'll receive a complaints response form. This will tell you about your right of appeal to the relevant Director, who will undertake an independent investigation and response within 10 working days should you wish them to do so.

What if I'm still not satisfied?

If you're still not satisfied, you can refer your complaint to the Chief Executive who, together with two Councillors, will undertake a full inquiry and give you their response within 10 working days.

What if I still don't agree with the Council?

You have the right to make your complaint about the Council to the Local Government Ombudsman. You can complain to the Ombudsman at any time but they won't usually start an investigation until we have been given the opportunity to put things right.

Will it make a difference?

Complaints are monitored and results will be published.

The complaints procedure and monitoring is co-ordinated by



Schedule 5 Extracts from Data Protection Act 1998 and Data Protection Code of Practice July 2000

Section 7

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

- (5) In subsection (4) the reference to information relating to another individual includes a reference to information identifying that individual as the source of the information sought by the request; and that subsection is not to be construed as excusing the Data Controller from communicating so much of the information sought by the request as can be communicated without disclosing the identity of the other individual concerned, whether by omission of names or other identifying particulars or otherwise.
- (6) In determining for the purposes of subsection (4)(b) whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned, regard shall be had, in particular, to:
- (a) any duty of confidentiality owed to the other individual,
 - (b) any steps taken by the Data Controller with a view to seeking the consent of the other individual,
 - (c) whether the other individual is capable of giving consent, and
 - (d) any express refusal of consent by the other individual.
- (7) An individual making a request under this section may, in such cases as may be prescribed, specify that his/her request is limited to personal data of any prescribed description.
- (8) Subject to subsection (4), a Data Controller shall comply with a request under this section promptly and in any event before the end of the prescribed period beginning with the relevant day.
- (9) If a court is satisfied on the application of any person who has made a request under the forgoing provisions of this section that the data controller in question has failed to comply with the request in contravention of those provisions, the court may order him/her to comply with the request.

In this section:

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

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

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

‘the relevant day’, in relation to a request under this section, means the day on which the data controller receives the request or, if later, the first day on which the data controller has both the required fee and the information referred to in subsection (3).

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

Section 8

- (1) The Secretary of State may by regulations provide that, in such cases as may be prescribed, a request for information under any provision of subsection (1) of section 7 is to be treated as extending also to information under other provisions of that subsection.
- (2) The obligation imposed by section 7(1)(c)(i) must be complied with by supplying the data subject with a copy of the information in permanent form unless:
- (a) the supply of such a copy is not possible or would involve disproportionate effort, or
 - (b) the data subject agrees otherwise;
 - (c) and where any of the information referred to in section 7(1)(c)(i) is expressed in terms which are not intelligible without explanation the copy must be accompanied by an explanation of those terms.

- (3) Where a Data Controller has previously complied with a request made under section 7 by an individual, the Data Controller is not obliged to comply with a subsequent identical or similar request under that section by that individual unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request.
- (4) In determining for the purposes of subsection (3) whether requests under section 7 are made at reasonable intervals, regard shall be had to the nature of the data, the purpose for which the data are processed and the frequency with which the data are altered.
- (5) Section 7(1)(d) is not to be regarded as requiring the provision of information as to the logic involved in decision-taking if, and to the extent that, the information constitutes a trade secret.
- (6) The information to be supplied pursuant to request under section 7 must be supplied by reference to the data in question at the time when the request is received, except that it may take account of any amendment or deletion made between that time and the time when the information is supplied, being an amendment or deletion that would have been made regardless of the receipt of the request.
- (7) For the purposes of section 7(4) and (5) another individual can be identified from the information being disclosed if he/she can be identified from that information, or from that and any other information which, in the reasonable belief of the Data Controller, is likely to be in, or to come into, the possession of the data subject making the request.

DATA PROTECTION CODE OF PRACTICE – JULY 2000

Foreword

Closed circuit television (CCTV) surveillance is an increasing feature of our daily lives. There is an ongoing debate over how effective CCTV is in reducing and preventing crime, but one thing is certain, its deployment is commonplace in a variety of areas to which members of the public have free access. We might be caught on camera while walking down the high street, visiting a shop or bank or travelling through a railway station or airport. The House of Lords Select Committee on Science and Technology expressed their view that if public confidence in CCTV systems was to be maintained there needed to be some tighter control over their deployment and use (5th Report - Digital Images as Evidence).

There was no statutory basis for systematic legal control of CCTV surveillance over public areas until 1st March 2000 when the Data Protection Act came into force. The definitions in this new Act are broader than those of the Data Protection Act 1984 and so more readily cover the processing of images of individuals caught by CCTV cameras than did the previous data protection legislation. The same legally enforceable information-handling standards as have previously applied to those processing personal data on computer now cover CCTV. An important new feature of the recent legislation is a power for me to issue a Commissioner's Code of Practice (section 51(3)(b) DPA '98) setting out guidance for the following of good practice. In my 14th Annual Report to Parliament I signalled my intention to use this power to provide guidance on the operation of CCTV as soon as those new powers became available to me. This Code of Practice is the first Commissioner's Code to be issued under the Data Protection Act 1998.

This code deals with surveillance in areas to which the public have largely free and unrestricted access because, as the House of Lords Committee highlighted, there is particular concern about a lack of regulation and central guidance in this area. Although the Data Protection Act 1998 covers other uses of CCTV this Code addresses the area of widest concern. Many of its provisions will be relevant to other uses of CCTV and will be referred to as appropriate when we develop other guidance. There are some existing standards that have been developed by representatives of CCTV system operators and, more particularly, the British Standards Institute. While such standards are helpful, they are not legally enforceable. The changes in data protection legislation mean that for the first time legally enforceable standards will apply to the collection and processing of images relating to individuals.

This Code of Practice has the dual purpose of assisting operators of CCTV systems to understand their legal obligations while also reassuring the public about the safeguards that should be in place. It sets out the measures which must be adopted to comply with the Data Protection Act 1998, and goes on to set out guidance for the following of good data protection practice. The Code makes clear the standards which must be followed to ensure compliance with the Data Protection Act 1998 and then indicates those which are not a strict legal requirement but do represent the following of good practice.

Before issuing this Code I consulted representatives of relevant data controllers and data subjects, and published a draft copy of the Code on my website. I am grateful to all those consultees who responded and have taken account of their comments in producing this version.

Our experience of the Codes of Practice that were put forward under the 1984 Act was that they needed to remain relevant to the day-to-day activities of data controllers. They need to be 'living' documents, which are updated as practices, and understanding of the law develops.

This code will therefore be kept under review to ensure that it remains relevant in the context of changing technology, use and jurisprudence. In this context it is likely that the Human Rights Act 1998, which comes into force on 2 October 2000, and provides important legal safeguards for individuals, will lead to developments in legal interpretation which will require review of the Code.

It is my intention that this Code of Practice should help those operating CCTV schemes monitoring members of the public to do so in full compliance of the Data Protection Act 1998 and in adherence to high standards of good practice. There does seem to be public support for the widespread deployment of this surveillance technology, but public confidence has to be earned and maintained. Compliance with this Code will not only help CCTV scheme operators' process personal data in compliance with the law but also help to maintain that public confidence without which they cannot operate.

Elizabeth France
Data Protection Commissioner
July 2000

Introduction

This is a code of practice issued by the Data Protection Commissioner in accordance with her powers under Section 51 (3)(b) of the Data Protection Act 1998 (the "1998 Act"). It is intended to provide guidance as to good practice for users of CCTV (closed circuit television) and similar surveillance equipment.

It is not intended that the contents of this Code should apply to: -

- Targeted and intrusive surveillance activities, which are covered by the provisions of the forthcoming Regulation of Investigatory Powers Act.
- Use of surveillance techniques by employers to monitor their employees' compliance with their contracts of employment.
- Security equipment (including cameras) installed in homes by individuals for home security purposes.
- Use of cameras and similar equipment by the broadcast media for the purposes of journalism, or for artistic or literary purposes.

This Code of Practice is drafted in two parts:

Part I

This sets out:

- the standards that must be met if the requirements of the 1998 Act are to be complied with. These are based on the Data Protection Principles which say that data must be
 - fairly and lawfully processed;
 - processed for limited purposes and not in any manner incompatible with those purposes;
 - adequate, relevant and not excessive;
 - accurate;
 - not kept for longer than is necessary
 - processed in accordance with individuals' rights;
 - secure;
 - not transferred to countries without adequate protection.
- guidance on good practice,
- examples of how to implement the standards and good practice.

The Data Protection Commissioner has the power to issue Enforcement Notices where she considers that there has been a breach of one or more of the Data Protection Principles. An Enforcement Notice would set out the remedial action that the Commissioner requires to ensure future compliance with the requirements of the Act. The Data Protection Commissioner will take into account the extent to which users of CCTV and similar surveillance equipment have complied with this Code of Practice when determining whether they have met their legal obligations when exercising her powers of enforcement.

Part II - Glossary

This sets out the interpretation of the 1998 Act on which Part I is based. Part I is cross-referenced to Part II to try to clarify the reasoning behind the standard or guidance.

It is intended that this Code of Practice will be revised on a regular basis in order to take account of developments in the interpretation of the provisions of the data protection legislation, developments in the technology involved in the recording of images, and developments in the use of such technologies, the use of sound recording, facial recognition techniques and the increased use of digital technology.

PART I

INITIAL ASSESSMENT PROCEDURES

Before installing and using CCTV and similar surveillance equipment, users will need to establish the purpose or purposes for which they intend to use the equipment. This equipment may be used for a number of different purposes – for example, prevention, investigation and detection of crime, apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings), public and employee safety, monitoring security of premises etc.

Standards

1. establish who is the person(s) or organisation(s) legally responsible for the proposed scheme.
2. assess the appropriateness of, and reasons for, using CCTV or similar surveillance equipment (First Data Protection Principle).
3. document this assessment process and the reasons for the installation of the scheme.
4. establish the purpose of the Scheme (First and Second Data Protection Principle).
5. document the purpose of the scheme.
6. ensure that the notification lodged with the Office of the Data Protection Commissioner covers the purposes for which this equipment is used
7. establish and document the person(s) or organisation(s) who are responsible for ensuring the day-to-day compliance with the requirements of this Code of Practice (if different from above)
8. establish and document security and disclosure policies.

SITING THE CAMERAS

It is essential that the location of the equipment is carefully considered, because the way in which images are captured will need to comply with the First Data Protection Principle. Detailed guidance on the interpretation of the First Data Protection Principle is provided in Part II, but the standards to be met under this Code of Practice are set out below.

Standards

1. The equipment should be sited in such a way that it only monitors those spaces that are intended to be covered by the equipment (First and Third Data Protection Principles).
2. If domestic areas such as gardens or areas not intended to be covered by the scheme border those spaces which are intended to be covered by the equipment, then the user should consult with the owners of such spaces if images from those spaces might be recorded. In the case of back gardens, this would be the resident of the property overlooked (First and Third Data Protection Principles).
3. Operators must be aware of the purpose(s) for which the scheme has been established (Second and Seventh Data Protection Principles).
4. Operators must be aware that they are only able to use the equipment in order to achieve the purpose(s) for which it has been installed (First and Second Data Protection Principles).

5. If cameras are adjustable by the operators, this should be restricted so that operators cannot adjust or manipulate them to overlook spaces that are not intended to be covered by the scheme (First and Third Data Protection Principles).
6. If it is not possible physically to restrict the equipment to avoid recording images from those spaces not intended to be covered by the scheme, then operators should be trained in recognising the privacy implications of such spaces being covered (First and Third Data Protection Principles).

For example – individuals sunbathing in their back gardens may have a greater expectation of privacy than individuals mowing the lawn of their front garden.

For example – it may be appropriate for the equipment to be used to protect the safety of individuals when using ATMs, but images of PIN numbers, balance enquiries etc should not be captured.

7. Signs should be placed so that the public are aware that they are entering a zone that is covered by surveillance equipment (First Data Protection Principle).
8. The signs should be clearly visible and legible to members of the public (First Data Protection Principle)
9. The size of signs will vary according to circumstances:

For example – a sign on the entrance door to a building society office may only need to be A4 size because it is at eye level of those entering the premises.

For example - signs at the entrances of car parks alerting drivers to the fact that the car park is covered by such equipment will usually need to be large, for example, probably A3 size as they are likely to be viewed from further away, for example by a driver sitting in a car.

10. The signs should contain the following information:
 - a) Identity of the person or organisation responsible for the scheme.
 - b) The purposes of the scheme.
 - c) Details of whom to contact regarding the scheme. (First Data Protection Principle)

For example - Where an image of a camera is not used on a sign – the following wording is recommended:

"Images are being monitored for the purposes of crime prevention and public safety. This scheme is controlled by the Greentown Safety Partnership.
For further information contact 01234-567-890"

For example – Where an image of a camera is used on a sign – the following wording is recommended:

"This scheme is controlled by the Greentown Safety Partnership.
For further information contact 01234-567-890"

11. In exceptional and limited cases, if it is assessed that the use of signs would not be appropriate, the user of the scheme must ensure that they have:
 - a) Identified specific criminal activity.
 - b) Identified the need to use surveillance to obtain evidence of that criminal activity.
 - c) Assessed whether the use of signs would prejudice success in obtaining such evidence.
 - d) Assessed how long the covert monitoring should take place to ensure that it is not carried out for longer than is necessary.
 - e) Documented (a) to (d) above.

12. Information so obtained must only be obtained for prevention or detection of criminal activity, or the apprehension and prosecution of offenders. It should not be retained and used for any other purpose. If the equipment used has a sound recording facility, this should not be used to record conversations between members of the public (First and Third Data Protection Principles).

QUALITY OF THE IMAGES

It is important that the images produced by the equipment are as clear as possible in order that they are effective for the purpose(s) for which they are intended. This is why it is essential that the purpose of the scheme is clearly identified. For example if a system has been installed to prevent and detect crime, then it is essential that the images are adequate for that purpose. The Third, Fourth and Fifth Data Protection Principles are concerned with the quality of personal data, and they are outlined in more detail in Part II. The standards to be met under this Code of Practice are set out below.

Standards

1. Upon installation, an initial check should be undertaken to ensure that the equipment performs properly.
2. If tapes are used, it should be ensured that they are good quality tapes (Third and Fourth Data Protection Principles).
3. The medium on which the images are captured should be cleaned so that images are not recorded on top of images recorded previously (Third and Fourth Data Protection Principles).
4. The medium on which the images have been recorded should not be used when it has become apparent that the quality of images has deteriorated. (Third Data Protection Principle).
5. If The System records features such as the location of the camera and/or date and time reference, these should be accurate (Third and Fourth Data Protection Principles).
6. If The System includes such features, users should ensure that they have a documented procedure for ensuring their accuracy.
7. Cameras should be situated so that they will capture images relevant to the purpose for which the scheme has been established (Third Data Protection Principle)

For example, if the purpose of the scheme is the prevention and detection of crime and/or apprehension and prosecution of offenders, the cameras should be sited so that images enabling identification of perpetrators are captured.

For example, if the scheme has been established with a view to monitoring traffic flow, the cameras should be situated so that they do not capture the details of the vehicles or drivers.

8. If an automatic facial recognition system is used to match images captured against a database of images, then both sets of images should be clear enough to ensure an accurate match (Third and Fourth Data Protection Principles).
9. If an automatic facial recognition system is used, procedures should be set up to ensure that the match is also verified by a human operator, who will assess the match and determine what action, if any, should be taken (First and Seventh Data Protection Principles).
10. The result of the assessment by the human operator should be recorded whether or not they determine there is a match.

11. When installing cameras, consideration must be given to the physical conditions in which the cameras are located (Third and Fourth Data Protection Principles).

For example – infrared equipment may need to be installed in poorly lit areas.

12. Users should assess whether it is necessary to carry out constant real time recording, or whether the activity or activities about which they are concerned occur at specific times (First and Third Data Protection Principles)

For example – it may be that criminal activity only occurs at night, in which case constant recording of images might only be carried out for a limited period e.g. 10.00 pm to 7.00 am

13. Cameras should be properly maintained and serviced to ensure that clear images are recorded (Third and Fourth Data Protection Principles)
14. Cameras should be protected from vandalism in order to ensure that they remain in working order (Seventh Data Protection Principle)
15. A maintenance log should be kept.
16. If a camera is damaged, there should be clear procedures for:
 - a) Defining the person responsible for making arrangements for ensuring that the camera is fixed.
 - b) Ensuring that the camera is fixed within a specific time period (Third and Fourth Data Protection Principle).
 - c) Monitoring the quality of the maintenance work.

PROCESSING THE IMAGES

Images which are not required for the purpose(s) for which the equipment is being used, should not be retained for longer than is necessary. While images are retained, it is essential that their integrity be maintained, whether it is to ensure their evidential value or to protect the rights of people whose images may have been recorded. It is therefore important that access to and security of the images is controlled in accordance with the requirements of the 1998 Act. The Seventh Data Protection Principle sets out the security requirements of the 1998 Data Protection Act. This is discussed in more depth at Part II. However, the standards required by this Code of Practice are set out below.

Standards

1. Images should not be retained for longer than is necessary (Fifth Data Protection Principle)

For example – publicans may need to keep recorded images for no longer than seven days because they will soon be aware of any incident such as a fight occurring on their premises.

For example – images recorded by equipment covering town centres and streets may not need to be retained for longer than 31 days unless they are required for evidential purposes in legal proceedings.

For example – images recorded from equipment protecting individuals' safety at ATMs might need to be retained for a period of three months in order to resolve customer disputes about cash withdrawals. The retention period of three months is based on the interval at which individuals receive their account statements.
2. Once the retention period has expired, the images should be removed or erased (Fifth Data Protection Principle).

3. If the images are retained for evidential purposes, they should be retained in a secure place to which access is controlled (Fifth and Seventh Data Protection Principles).
4. On removing the medium on which the images have been recorded for the use in legal proceedings, the operator should ensure that they have documented:
 - a) The date on which the images were removed from the general system for use in legal proceedings.
 - b) The reason why they were removed from The System.
 - c) Any crime incident number to which the images may be relevant.
 - d) The location of the images.

For example- if the images were handed to a Police Officer for retention, the name and station of that Police Officer.

- e) The signature of the collecting Police Officer, where appropriate (see below)(Third and Seventh Data Protection Principles).
5. Monitors displaying images from areas in which individuals would have an expectation of privacy should not be viewed by anyone other than authorised employees of the user of the equipment (Seventh Data Protection Principle).
6. Access to the recorded images should be restricted to a manager or designated member of staff who will decide whether to allow requests for access by third parties in accordance with the user's documented disclosure policies (Seventh Data Protection Principle).
7. Viewing of the recorded images should take place in a restricted area, for example, in a manager's or designated member of staff's office. Other employees should not be allowed to have access to that area when a viewing is taking place (Seventh Data Protection Principle).
8. Removal of the medium on which images are recorded, for viewing purposes, should be documented as follows:
 - a) The date and time of removal
 - b) The name of the person removing the images
 - c) The name(s) of the person(s) viewing the images. If this should include third parties, this include the organisation of that third party
 - d) The reason for the viewing
 - e) The outcome, if any, of the viewing
 - f) The date and time the images were returned to The System or secure place, if they have been retained for evidential purposes
9. All operators and employees with access to images should be aware of the procedure which need to be followed when accessing the recorded images (Seventh Data Protection Principle).
10. All operators should be trained in their responsibilities under this Code of Practice i.e. they should be aware of:
 - a) The user's security policy e.g. procedures to have access to recorded images.
 - b) The user's disclosure policy.
 - c) Rights of individuals in relation to their recorded images. (Seventh Data Protection Principle)

ACCESS TO AND DISCLOSURE OF IMAGES TO THIRD PARTIES

It is important that access to, and disclosure of, the images recorded by CCTV and similar surveillance equipment is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes. Users of CCTV will also need to ensure that the reason(s) for which they may disclose copies of the images are compatible with the reason(s) or purpose(s) for which they originally obtained those images. These aspects of this Code are to be found in the Second and Seventh Data Protection Principles, which are discussed in more depth at Part II. However, the standards required by this Code are set out below.

Standards

All employees should be aware of the restrictions set out in this Code of Practice in relation to access to, and disclosure of, recorded images.

1. Access to recorded images should be restricted to those staff who need to have access in order to achieve the purpose(s) of using the equipment (Seventh Data Protection Principle).
2. All access to the medium on which the images are recorded should be documented (Seventh Data Protection Principle).
3. Disclosure of the recorded images to third parties should only be made in limited and prescribed circumstances (Second and Seventh Data Protection Principles).

For example - if the purpose of The System is the prevention and detection of crime, then disclosure to third parties should be limited to the following:

- Law enforcement agencies where the images recorded would assist in a specific criminal enquiry
 - Prosecution agencies
 - Relevant legal representatives
 - The media, where it is decided that the public's assistance is needed in order to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. As part of that decision, the wishes of the victim of an incident should be taken into account
 - People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings)
4. All requests for access or for disclosure should be recorded. If access or disclosure is denied, the reason should be documented (Seventh Data Protection Principle)
 5. If access to or disclosure of the images is allowed, then the following should be documented:
 - a) The date and time at which access was allowed or the date on which disclosure was made
 - b) The identification of any third party who was allowed access or to whom disclosure was made
 - c) The reason for allowing access or disclosure
 - d) The extent of the information to which access was allowed or which was disclosed
 6. Recorded images should not be made more widely available - for example they should not be routinely made available to the media or placed on the Internet (Second, Seventh and Eighth Data Protection Principles).

7. If it is intended that images will be made more widely available, that decision should be made by the manager or designated member of staff. The reason for that decision should be documented (Seventh Data Protection Principle).
8. If it is decided that images will be disclosed to the media (other than in the circumstances outlined above), the images of individuals will need to be disguised or blurred so that they are not readily identifiable (First, Second and Seventh Data Protection Principles).
9. If The System does not have the facilities to carry out that type of editing, an editing company may need to be hired to carry it out.
10. If an editing company is hired, then the manager or designated member of staff needs to ensure that:
 - a) There is a contractual relationship between the data controller and the editing company.
 - b) That the editing company has given appropriate guarantees regarding the security measures they take in relation to the images.
 - c) The manager has checked to ensure that those guarantees are met
 - d) The written contract makes it explicit that the editing company can only use the images in accordance with the instructions of the manager or designated member of staff.
 - e) The written contract makes the security guarantees provided by the editing company explicit. (Seventh Data Protection Principle)
11. If the media organisation receiving the images undertakes to carry out the editing, then (a) to (e) will still apply (Seventh Data Protection Principle)

ACCESS BY DATA SUBJECTS

This is a right, which is provided by section 7 of the 1998 Act. A detailed explanation of the interpretation of this right is given in Part II. The standards of this Code of Practice are set out below.

Standards

1. All staff involved in operating the equipment must be able to recognise a request for access to recorded images by data subjects (Sixth and Seventh Data Protection Principles).
2. Data subjects should be provided with a standard subject access request form which:
 - a) Indicates the information required in order to locate the images requested.
For example – an individual may have to provide dates and times of when they visited the premises of the user of the equipment.
 - b) Indicates the information required in order to identify the person making the request.
For example –if the individual making the request is unknown to the user of the equipment, a photograph of the individual may be requested in order to locate the correct image.
 - c) Indicates the fee that will be charged for carrying out the search for the images requested. A maximum of £10.00 may be charged for the search.
 - d) Asks whether the individual would be satisfied with merely viewing the images recorded.
 - e) Indicates that the response will be provided promptly and in any event within 40 days of receiving the required fee and information.
 - f) Explains the rights provided by the 1998 Act.
3. Individuals should also be provided with a leaflet which describes the types of images which are recorded and retained, the purposes for which those images are recorded and retained, and information about the disclosure policy in relation to those images (Sixth Data Protection Principle).

4. This should be provided at the time that the standard subject access request form is provided to an individual (Sixth Data Protection Principle).
5. All subject access requests should be dealt with by a manager or designated member of staff.
6. The manager or designated member of staff should locate the images requested
7. The manager or designated member of staff should determine whether disclosure to the individual would entail disclosing images of third parties (Sixth Data Protection Principle).
8. The manager or designated member of staff will need to determine whether the images of third parties are held under a duty of confidence (First and Sixth Data Protection Principle).

For example - it may be that members of the public whose images have been recorded when they were in town centres or streets have less expectation that their images are held under a duty of confidence than individuals whose images have been recorded in more private space such as the waiting room of a doctor's surgery.

9. If third party images are not to be disclosed, the manager or designated member of staff shall arrange for the third party images to be disguised or blurred (Sixth Data Protection Principle).
10. If the system does not have the facilities to carry out that type of editing, a third party or company may be hired to carry it out
11. If a third party or company is hired, then the manager or designated member of staff needs to ensure that:
 - a) There is a contractual relationship between the Data Controller and the third party or company.
 - b) That the third party or company has given appropriate guarantees regarding the security measures they take in relation to the images.
 - c) The manager has checked to ensure that those guarantees are met.
 - d) The written contract makes it explicit that the third party or company can only use the images in accordance with the instructions of the manager or designated member of staff.
 - e) The written contract makes the security guarantees provided by the third party or company explicit
(Seventh Data Protection Principle)
12. If the manager or designated member of staff decides that a subject access request from an individual is not to be complied with, the following should be documented:
 - a) The identity of the individual making the request
 - b) The date of the request
 - c) The reason for refusing to supply the images requested
 - d) The name and signature of the manager or designated member of staff making the decision.
13. All staff should be aware of individuals' rights under this section of the Code of Practice (Seventh Data Protection Principle)

OTHER RIGHTS

A detailed explanation of the other rights under Sections 10, 12 and 13 of the Act are provided in Part II of this Code. The standards of this Code are set out below.

Standards

1. All staff involved in operating the equipment must be able to recognise a request from an individual to:
 - a) Prevent processing likely to cause substantial and unwarranted damage to that individual.
 - b) Prevent automated decision taking in relation to that individual.
2. All staff must be aware of the manager or designated member of staff who is responsible for responding to such requests.
3. In relation to a request to prevent processing likely to cause substantial and unwarranted damage, the manager or designated officer's response should indicate whether he or she will comply with the request or not.
4. The manager or designated member of staff must provide a written response to the individual within 21 days of receiving the request setting out their decision on the request.
5. If the manager or designated member of staff decide that the request will not be complied with, they must set out their reasons in the response to the individual.
6. A copy of the request and response should be retained.
7. If an automated decision is made about an individual, the manager or designated member of staff must notify the individual of that decision.
8. If, within 21 days of that notification, the individual requires, in writing, the decision to be reconsidered, the manager or designated staff member shall reconsider the automated decision.
9. On receipt of a request to reconsider the automated decision, the manager or designated member of staff shall respond within 21 days setting out the steps that they intend to take to comply with the individual's request.
10. The manager or designated member of staff shall document:
 - a) The original decision.
 - b) The request from the individual.
 - c) Their response to the request from the individual.

MONITORING COMPLIANCE WITH THIS CODE OF PRACTICE

Standards

1. The contact point indicated on the sign should be available to members of the public during office hours. Employees staffing that contact point should be aware of the policies and procedures governing the use of this equipment.
2. Enquiries should be provided on request with one or more of the following:
 - a) The leaflet which individuals receive when they make a subject access request as general information
 - b) A copy of this Code of Practice
 - c) A subject access request form if required or requested
 - d) The complaints procedure to be followed if they have concerns about the use of the system
 - e) The complaints procedure to be followed if they have concerns about non-compliance with the provisions of this Code of Practice
3. A complaints procedure should be clearly documented.
4. A record of the number and nature of complaints or enquiries received should be maintained together with an outline of the action taken.
5. A report on those numbers should be collected by the manager or designated member of staff in order to assess public reaction to and opinion of the use of the system.
6. A manager or designated member of staff should undertake regular reviews of the documented procedures to ensure that the provisions of this Code are being complied with (Seventh Data Protection Principle).
7. A report on those reviews should be provided to the data controller(s) in order that compliance with legal obligations and provisions with this Code of Practice can be monitored.
8. An internal annual assessment should be undertaken which evaluates the effectiveness of the system.
9. The results of the report should be assessed against the stated purpose of the scheme. If the scheme is not achieving its purpose, it should be discontinued or modified.
10. The result of those reports should be made publicly available.

PART II

GLOSSARY

THE DATA PROTECTION ACT 1998

1. DEFINITIONS

There are several definitions in Sections 1 and 2 of the 1998 Act which users of CCTV systems or similar surveillance equipment must consider in order to determine whether they need to comply with the requirements of the 1998 Act, and if so, to what extent the 1998 Act applies to them:

a) Data Controller

“A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed”.

For example- if a police force and local authority enter into a partnership to install CCTV in a town centre with a view to: -

- Preventing and detecting crime.
- Apprehending and prosecuting offenders.
- Protecting public safety.

They will both be data controllers for the purpose of the scheme.

For example- if a police force, local authority and local retailers decide to install a CCTV scheme in a town centre or shopping centre, for the purposes of:

- Prevention or detection crime.
- Apprehending or prosecuting offenders.
- Protecting public safety.

All will be data controllers for the purposes of the scheme. It is the data controllers who should set out the purposes of the scheme (as outlined above) and who should set out the policies on the use of the images (as outlined in the Standards section of this Code of Practice).

The data controller(s) may devolve day-to-day running of the scheme to a manager, but that manager is not the data controller - he or she can only manage the scheme according to the instructions of the data controller(s), and according to the policies set out by the data controller(s).

If the manager of the scheme is an employee of one or more of the data controllers, then the manager will not have any personal data protection responsibilities as a data controller. However, the manager should be aware that if he or she acts outside the instructions of the data controller(s) in relation to obtaining or disclosing the images, they may commit a criminal offence contrary to Section 55 of the 1998 Act, as well as breach their contract of employment.

If the manager is a third party such as a security company employed by the data controller to run the scheme, then the manager may be deemed a data processor. This is “any person (other than an employee of the data controller) who processes the personal data on behalf of the data controller. If the data controller(s) are considering using a data processor, they will need to consider their compliance with the Seventh Data Protection Principle in terms of this relationship.

b) Personal Data

“Data that relate to a living individual who can be identified:

- a) from those data, or
- b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller”.

The provisions of the 1998 Act are based on the requirements of a European Directive, which at, Article 2, defines, personal data as follows:

“Personal data” shall mean any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

The definition of personal data is not therefore limited to circumstances where a data controller can attribute a name to a particular image. If images of distinguishable individuals’ features are processed and an individual can be identified from these images, they will amount to personal data.

c) Sensitive Personal Data

Section 2 of the 1998 Act separates out distinct categories of personal data, which are deemed sensitive. The most significant of these categories for the purposes of this code of practice are information about:

- the commission or alleged commission of any offences
- any proceedings for any offence committed, or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

This latter bullet point will be particularly significant for those CCTV schemes which are established by retailers in conjunction with the local police force, which use other information to identify known and convicted shoplifters from images, with a view to reducing the amount of organised shoplifting in a retail centre.

It is essential that data controllers determine whether they are processing sensitive personal data because it has particular implications for their compliance with the First Data Protection Principle.

d) Processing

Section I of the 1998 Act sets out the type of operations that can constitute processing:

"In relation to information or data, means obtaining, processing, 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."

The definition is wide enough to cover the simple recording and holding of images for a limited period of time, even if no further reference is made to those images. It is also wide enough to cover real-time transmission of the images. Thus if the images of individuals passing in front of a camera are shown in real time on a monitor, this constitutes “transmission, dissemination or otherwise making available. Thus even the least sophisticated capturing and use of images falls within the definition of processing in the 1998 Act.

2. PURPOSES FOR WHICH PERSONAL DATA/IMAGES ARE PROCESSED

Before considering compliance with the Data Protection Principles, a user of CCTV or similar surveillance equipment, will need to determine two issues:

- What type of personal data are being processed i.e. are there any personal data which fall within the definition of sensitive personal data as defined by Section 2 of the 1998 Act.
- For what purpose(s) are both personal data and sensitive personal data being processed?

Users of surveillance equipment should be clear about the purposes for which they intend to use the information/images captured by their equipment. The equipment may be used for a number of purposes:

- Prevention, investigation and/or detection of crime.
- Apprehension and/or prosecution of offenders (including images being entered as evidence in criminal proceedings).
- Public and employee safety.
- Staff discipline.
- Traffic flow monitoring.

Using information captured by a surveillance system will not always require the processing of personal data or the processing of sensitive personal data. For example, use of the system to monitor traffic flow in order to provide the public with up to date information about traffic jams, will not necessarily require the processing of personal data.

3. DATA PROTECTION PRINCIPLES

THE FIRST DATA PROTECTION PRINCIPLE

This requires that

“Personal data shall be processed fairly and lawfully, and, in particular, shall not be processed unless:

- a) at least one of the conditions in Schedule 2 is met, and
- b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met”.

To assess compliance with this Principle, it is recommended that the data controller address the following questions:

a) Are personal data and/or sensitive personal data processed?

The definition of sensitive personal data has been discussed above and it is essential that the data controller has determined whether they are processing information/images, which

fall into that category in order to assess which criteria to consider when deciding whether there is a legitimate basis for the processing of that information/images.

b) Has a condition for processing been met?

The First Data Protection Principle requires that the *data controller* have a legitimate basis for processing. It is for the data controller to be clear about which grounds to rely on in this respect. These are set out in Schedules 2 and 3 to the Act.

Users of schemes which monitor spaces to which the public have access, such as town centres, may be able to rely on Paragraph 5 (d) of Schedule 2 because the processing is for the exercise of any other function of a public nature exercised in the public interest by any person. This could include purposes such as prevention and detection of crime, apprehension and prosecution of offenders or public/employee safety.

Users of schemes which monitor spaces in shops or retail centres to which the public have access may be able to rely on Paragraph 6(l) of Schedule 2 because the processing is necessary for the purposes of legitimate interests pursued by the data controller or the third party or third parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

It should be noted that while this criterion may provide a general ground for processing, in an individual case, the interests of the data controller i.e. the user of the surveillance equipment might not outweigh the rights of an individual.

If the data controller has determined that he or she is processing sensitive personal data, then the data controller will also need to determine whether he or she has a legitimate basis for doing so under Schedule 3. It should be noted that Schedule 3 does not contain the grounds cited above in relation to Schedule 2.

Users of surveillance equipment in town centres, particularly where the local authority or police force (or a partnership of the two) are the data controllers may be able to rely on Paragraph 7(l)(b) of Schedule 3 because the processing is necessary for the exercise of any functions conferred on any person by or under an enactment. It may be that the use of such information/images by a public authority in order to meet the objectives of the Crime and Disorder Act 1998 would satisfy this criterion.

Users of information/images recorded in a shop or retail centre may be able to rely on one of the grounds contained in the Order made under Schedule 3(10) of the 1998 Act.

For example-

“(1) The processing:

- a) is in the substantial public interest;
- b) is necessary for the purposes of the prevention and detection of any unlawful act; and
- c) must necessarily be carried out without the explicit consent of the data subject so as not to prejudice those purposes”

It is for the data controller to be sure that he or she has legitimate grounds for their processing and therefore it is essential that the data controller has identified:

- what categories of data are processed, and
- why.

c) Are the information/images processed lawfully?

The fact that the data controller has a legitimate basis for processing does not mean that this element of the First Data Protection Principle is automatically satisfied. The data controller will also need to consider whether the information/images processed are subject to any other legal duties or responsibilities such as the common law duty of confidentiality. Public sector bodies will need to consider their legal powers under administrative law in order to determine whether there are restrictions or prohibitions on their ability to process such data. They will also need to consider the implications of the Human Rights Act 1998.

d) Are the information/images processed fairly?

The fact that a data controller has a legitimate basis for processing the information/images will not automatically mean that this element of the First Data Protection Principle is satisfied.

The interpretative provisions of the Act set out what is required in order to process fairly. In order to process fairly, the following information, at least, must be provided to the individuals at the point of obtaining their images:

- the identity of the data controller
- the identity of a representative the data controller has nominated for the purposes of the Act
- the purpose or purposes for which the data are intended to be processed, and
- any information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the individual to be fair.

e) Circumstances in which the requirement for signs may be set aside

The Act does not make specific reference to the use of covert processing of (sensitive) personal data but it does provide a limited exemption from the requirement of fair processing. Because fair processing (as indicated above) requires that individuals are made aware that they are entering an area where their images may be captured, by the use of signs, it follows that the use of covert processing i.e. removal or failure to provide signs, is prima facie a breach of the fairness requirement of the First Data Protection Principle. However, a breach of this requirement will not arise if an exemption can be relied on. Such an exemption may be found at Section 29(l) of the Act, which states that:

“Personal data processed for any of the following purposes:

- a) prevention or detection of crime
- b) apprehension or prosecution of offenders

are exempt from the first data protection principle (except to the extent to which it requires compliance with the conditions in Schedules 2 and 3) ... 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...”

This means that if the data controller processes images for either or both of the purposes listed in the exemption, he or she may be able to obtain and process images without signs without breaching the fairness requirements of the First Data Protection Principle.

THE SECOND DATA PROTECTION PRINCIPLE

This requires that

“Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes”.

In order to ascertain whether the data controller can comply with this Data Protection Principle, it is essential that he or she is clear about the purpose(s) for which the images are processed.

Specified purposes may be those, which have been notified to the Commissioner or to the individuals.

There are a number of issues to be considered when determining lawfulness:

- Whether the data controller has a legitimate basis (see First Data Protection Principle) for the processing.
- Whether the images are processed in accordance with any other legal duties to which the data controller may be subject e.g. the common law duty of confidence, administrative law in relation to public sector powers etc.

It is quite clear from the interpretative provisions to the Principle that the requirement of compatibility is particularly significant when considering making a disclosure to a third party or developing a policy on disclosures to third parties. If the data controller intends to make a disclosure to a third party, regard must be had to the purpose(s) for which the third party may process the data.

This means, for example, that if the purpose(s) for which images are processed is:

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

The data controller may only disclose to third parties who intend processing the data for compatible purposes. Thus, for example, where there is an investigation into criminal activity, disclosure of footage relating to that criminal activity to the media in order to seek assistance from the public in identifying either the perpetrator, the victim or witnesses, may be appropriate. However, it would be an incompatible use if images from equipment installed to prevent or detect crime were disclosed to the media merely for entertainment purposes. For example, it might be appropriate to disclose to the media images of drunken individuals stumbling around a town centre on a Saturday night to show proper use of policing resources to combat anti-social behaviour. However, it would not be appropriate for the same images to be provided to a media company merely for inclusion in a “humorous” video.

If it is determined that a particular disclosure is compatible with the purposes for which the data controller processes images, then the extent of disclosure will need to be considered. If the footage, which is to be disclosed contains images of unrelated third parties, the data controller will need to ensure that those images are disguised in such a way that they cannot be identified.

If the data controller does not have the facilities to carry out such editing, he or she may agree with the media organisation that it will ensure that those images are disguised. This will mean that the media organisation is carrying out processing, albeit of a limited nature on behalf of the data controller which is likely to render it a data processor. In which case the data controller will need to ensure that the relationship with the media organisation complies with the Seventh Data Protection Principle.

THE THIRD DATA PROTECTION PRINCIPLE

This requires that

“Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed”.

This means that consideration must be given to the situation of the cameras so that they do not record more information than is necessary for the purpose for which they were installed. For example cameras installed for the purpose of recording acts of vandalism in a car park should not overlook private residences. Furthermore, if the recorded images on the tapes are blurred or indistinct, it may well be that this will constitute inadequate data. For example, if the purpose of the system is to collect evidence of criminal activity, blurred or indistinct images from degraded tapes or poorly maintained equipment will not provide legally sound evidence, and may therefore be inadequate for its purpose.

THE FOURTH DATA PROTECTION PRINCIPLE

This requires that

“Personal data shall be accurate and, where necessary, kept up to date”.

This principle requires that the personal information that is recorded and stored must be accurate. This is particularly important if the personal information taken from the system is to be used as evidence in cases of criminal conduct or in disciplinary disputes with employees. The Commissioner recommends that efforts are made to ensure the clarity of the images, such as using only good quality tapes in recording the information, cleaning the tapes prior to re-use and not simply recording over existing images, and replacing tapes on a regular basis to avoid degradation from over-use.

If the data controller’s system uses features such as time references and even location references, then these should be accurate. This means having a documented procedure to ensure the accuracy of such features are checked and if necessary, amended or altered.

Care should be exercised when using digital-enhancement and compression technologies to produce stills for evidence from tapes because these technologies often contain pre-programmed presumptions as to the likely nature of sections of the image. Thus the user cannot be certain that the images taken from the tape are an accurate representation of the actual scene. This may create evidential difficulties if they are to be relied on either in court or an internal employee disciplinary hearing.

THE FIFTH DATA PROTECTION PRINCIPLE

This requires that

“Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes”.

This principle requires that the information shall not be held for longer than is necessary for the purpose for which it is to be used. The tapes that have recorded the relevant activities should be retained until such time as the proceedings are completed and the possibility of any appeal has been exhausted. After that time, the tapes should be erased. Apart from those circumstances, stored or recorded images should not be kept for any undue length of time. A policy on periods for retention of the images should be developed which takes into account the nature of the information and the purpose for which it is being collected. For example where images are being recorded for the purposes of crime prevention in a shopping area, it may be that the only images that need to be retained are those relating to specific incidents of criminal activity; the rest could be erased after a very short period. The

Commissioner understands that generally town centre schemes do not retain recorded images for more than 28 days unless the images are required for evidential purposes.

THE SIXTH DATA PROTECTION PRINCIPLE

This requires that

“Personal data shall be processed in accordance with the rights of data subjects under this Act”.

The Act provides individuals with a number of rights in relation to the processing of their personal data. Contravening the following rights will amount to a contravention of the Sixth Data Protection Principle:

- The right to be provided, in appropriate cases, with a copy of the information constituting the personal data held about them - Section 7.
- The right to prevent processing that is likely to cause damage or distress - Section 10.
- Rights in relation to automated decision-taking - Section 12

THE SEVENTH DATA PROTECTION PRINCIPLE

This requires that

“Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data”.

In order to assess the level of security the data controller needs to take to ensure compliance with this Principle, he or she needs to assess: -

- the harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage of the personal data. While it is clear that breach of this Principle may have a detrimental effect on the purpose(s) of the scheme e.g. the evidence or images might not stand up in court, or the public may lose confidence in your use of surveillance equipment due to inappropriate disclosure, the harm test required by the Act also requires primarily the effect on the people recorded to be taken into account;
- the nature of the data to be protected must be considered. Sensitive personal data was defined at the beginning of this part of the Code, but there may be other aspects, which need to be considered. For example, a town centre scheme may coincidentally record the image of a couple kissing in a parked car, or a retailer’s scheme may record images of people in changing rooms (in order to prevent items of clothing being stolen). Whilst these images may not fall within the sensitive categories as set in Section 2 (described above), it is clear that the people whose images have been captured will consider that information or personal data should be processed with greater care.

THE EIGHTH DATA PROTECTION PRINCIPLE

This requires that

“Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data”.

This Principle places limitations on the ability to transfer personal data to countries and territories outside of the EEA. It is unlikely that the data controller would want, in general, to make such transfers of personal data overseas, but the data controller should refrain from

putting the images on the Internet or on their website. In order to ensure that this Principle is not breached, the data controller should consider the provisions of Schedule 4 of the 1998 Act.

4. RIGHT OF SUBJECT ACCESS

Upon making a request in writing (which includes transmission by electronic means) and upon paying the fee to the data controller an individual is entitled:

- To be told by the data controller whether they or someone else on their behalf is processing that individual's personal data.
- If so, to be given a description of:
 - a) the personal data,
 - b) the purposes for which they are being processed, and
 - c) those to whom they are or may be disclosed.
- To be told, in an intelligible manner, of:
 - d) all the information, which forms any such personal data. This information must be supplied in permanent form by way of a copy, except where the supply of such a copy is not possible or would involve disproportionate effort or the individual agrees otherwise. If any of the information in the copy is not intelligible without explanation, the individual should be given an explanation of that information, e.g. where the data controller holds the information in coded form which cannot be understood without the key to the code, and
 - e) any information as to the source of those data. However, in some instances the data controller is not obliged to disclose such information where the source of the data is, or can be identified as, an individual.

A data controller may charge a fee (subject to a maximum) for dealing with subject access. A data controller must comply with a subject access request promptly, and in any event within forty days of receipt of the request or, if later, within forty days of receipt of:

- the information required (i.e. to satisfy himself as to the identity of the person making the request and to locate the information which that person seeks); and
- the fee.

However, unless the data controller has received a request in writing, the prescribed fee and, if necessary, the said information the data controller need not comply with the request. If the data controller receives a request without the required fee and/or information, they should request whichever is outstanding as soon as possible in order that they can comply with the request promptly and in any event within 40 days. A data controller does not need to comply with a request where they have already complied with an identical or similar request by the same individual unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request. In deciding what amounts to a reasonable interval, the following factors should be considered: the nature of the data, the purpose for which the data are processed and the frequency with which the data are altered.

The information given in response to a subject access request should be all that which is contained in the personal data at the time the request was received. However, routine amendments and deletions of the data may continue between the date of the request and the date of the reply. To this extent, the information revealed to the individual may differ from the personal data which were held at the time the request was received, even to the extent that data are no longer held. But, having received a request, the data controller must not make

any special amendment or deletion which would not otherwise have been made. The information must not be tampered with in order to make it acceptable to the individual.

A particular problem arises for data controllers who may find that in complying with a subject access request they will disclose information relating to an individual other than the individual who has made the request, who can be identified from that information, including the situation where the information enables that other individual to be identified as the source of the information. The Act recognises this problem and sets out only two circumstances in which the data controller is obliged to comply with the subject access request in such circumstances, namely:

- where the other individual has consented to the disclosure of the information, or
- where it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

The Act assists in interpreting whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned. In deciding this question regard shall be had, in particular, to:

- any duty of confidentiality owed to the other individual,
- any steps taken by the data controller with a view to seeking the consent of the other individual,
- whether the other individual is capable of giving consent, and
- any express refusal of consent by the other individual.

If a data controller is satisfied that the individual will not be able to identify the other individual from the information, taking into account 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 individual, then the data controller must provide the information.

If an individual believes that a data controller has failed to comply with a subject access request in contravention of the Act they may apply to Court for an order that the data controller complies with the request. An order may be made if the Court is satisfied that the data controller has failed to comply with the request in contravention of the Act.

5. EXEMPTIONS TO SUBJECT ACCESS RIGHTS

There are a limited number of exemptions to an individual's right of access. One of potential relevance to CCTV images is found at Section 29 of the Act. This provides an exemption from the subject access rights, which is similar to that discussed in relation to the exemption to the fairness requirements of the First Data Protection Principle. This means that where personal data are held for the purposes of:

- prevention or detection of crime,
- apprehension or prosecution of offenders,

the data controller will be entitled to withhold personal data from an individual making a subject access request, where it has been adjudged that to disclose the personal data would be likely to prejudice one or both of the above purposes. Like the exemption to the fairness requirements of the First Data Protection Principle, this judgement must be made on a case-by-case basis, and in relation to each element of the personal data held about the individual. It is likely that this exemption may only be appropriately relied upon where the data controller has recorded personal data about an individual in accordance with guidance set out in relation to the fairness requirements of the First Data Protection Principle.

6. OTHER RIGHTS

Right to Prevent Processing Likely to Cause Damage or Distress

Under Section 10 of the Act, an individual is entitled to serve a notice on a data controller requiring the data controller not to begin, or to cease, processing personal data relating to that individual. Such a notice could only be served on the grounds that the processing in question is likely to cause substantial, unwarranted damage or distress to that individual or another person. There are certain limited situations where this right to serve a notice does not apply. These are where the individual has consented; the processing is in connection with performance of a contract with the data subject, or in compliance with a legal obligation on the data controller, or in order to protect the vital interests of the individual. If a data controller receives such a notice they must respond within 21 days indicating either compliance with the notice or why the notice is not justified.

Rights in Relation to Automated Decision-Taking

Under section 12 of the Act individuals also have certain rights to prevent automated decision taking where a decision, which significantly affects them is based solely on automated processing. The Act draws particular attention to decisions taken aimed at evaluating matters such as the individual's performance at work and their reliability or conduct. The Act does provide exemption for certain decisions reached by automated means and these cover decisions which have been taken in the course of contractual arrangements with the individual, where a decision is authorised or required by statute, where the decision is to grant a request of the individual or where steps have been taken to safeguard the legitimate interests of individuals. This latter point may include matters such as allowing them to make representations about a decision before it is implemented.

Where no notice has been served by an individual and a decision which significantly affects the individual based solely on automated processing will be made, then there is still an obligation on the data controller to notify the individual that the decision was taken on the basis of automated processing as soon as reasonably practicable. The individual may, within 21 days of receiving such a notification, request the data controller to reconsider the decision or take another decision on a new basis. Having received such a notice the data controller has 21 days in which to respond, specifying the steps that they intend to take to comply with the notice.

In the context of CCTV surveillance it may be the case that certain automated decision-making techniques are deployed, such as with automatic facial recognition. It is important therefore that any system takes account of an individual's rights in relation to automated decision taking. It should be noted that these rights are founded on decisions, which are taken solely on the basis of automated processing. If a decision whether to take particular action in relation to a particular identified individual is taken further to human intervention, then such a decision would not be based solely on automated processing.

The individual's rights to prevent processing in certain circumstances and in connection with automated decision taking are underpinned by an individual's right to seek a Court Order should any notice served by the individual not be complied with.

Compensation for Failure to Comply with Certain Requirements

Under Section 13 of the Act, individuals who suffer unwarranted damage or damage and distress as a result of any contravention of the requirements of the Act are entitled to go to court to seek compensation in certain circumstances. This right to claim compensation for a breach of the Act is in addition to an individual's right to request the Data Protection Commissioner to make an assessment as to whether processing is likely or unlikely to comply with the Act.

Appendix A National Standard for the Release of Data to Third Parties

1. Introduction

Arguably CCTV is one of the most powerful tools to be developed during recent years to assist with efforts to combat crime and disorder whilst enhancing community safety. Equally it may be regarded by some as the most potent infringement of people's liberty. If users, owners and managers of such systems are to command the respect and support of the general public, the systems must not only be used with the utmost probity at all times, they must be used in a manner which stands up to scrutiny and is accountable to the very people they are aiming to protect.

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

2. General Policy

All requests for the release of data shall be processed in accordance with the Operational Procedures. All such requests shall be channelled through the Commissioning Officer (CCTV).

3. Primary Request To View Data

- a) Primary requests to view data generated by a CCTV System are likely to be made by third parties for any one or more of the following purposes:
 - i) Providing evidence in criminal proceedings (e.g. Police and Criminal Evidence Act 1984, Criminal Procedures & Investigations Act 1996, etc.);
 - ii) Providing evidence in civil proceedings or tribunals
 - iii) The prevention of crime
 - iv) The investigation and detection of crime (may include identification of offenders)
 - v) Identification of witnesses
- b) Third parties, which are required to show adequate grounds for disclosure of data within the above criteria, may include, but are not limited to:
 - i) Police
 - ii) Statutory authorities with powers to prosecute, (e.g. Customs and Excise; Trading Standards, etc.)
 - iii) Solicitors
 - iv) Plaintiffs in civil proceedings⁽³⁾
 - v) Accused persons or defendants in criminal proceedings
 - iv) Other agencies, (which should be specified in The Code) according to purpose and legal status.
- c) Upon receipt from a third party of a bona fide request for the release of data, the data controller shall:
 - i) Not unduly obstruct a third party investigation to verify the existence of relevant data.

- ii) Ensure the retention of data which may be relevant to a request, but which may be pending application for, or the issue of, a court order or subpoena. A time limit shall be imposed on such retention, which will be notified at the time of the request.
- d) On requests by plaintiffs, accused persons or defendants the data controller, or nominated representative, shall:
 - i) Be satisfied that there is no connection with any existing data held by the police in connection with the same investigation.
 - ii) Treat all such enquiries with strict confidentiality.

4. Secondary Request To View Data

- a) A 'secondary' request for access to data may be defined as any request being made which does not fall into the category of a primary request. Before complying with a secondary request, the data controller shall ensure that:
 - i) The request does not contravene, and that compliance with the request would not breach, current relevant legislation, (e.g. Data Protection Act 1998, Human Rights Act 1998, section 163 Criminal Justice and Public Order Act 1994, etc.);
 - ii) Any legislative requirements have been complied with, (e.g. the requirements of the Data Protection Act 1998);
 - iii) Due regard has been taken of any known case law (current or past) which may be relevant, (e.g. R v Brentwood BC ex p. Peck) and
 - iv) The request would pass a test of 'disclosure in the public interest'.
- b) If, in compliance with a secondary request to view data, a decision is taken to release material to a third party, the following safeguards shall be put in place before surrendering the material:
 - i) In respect of material to be released under the auspices of 'crime prevention', written agreement to the release of the material should be obtained from a Police Officer, not below the rank of Inspector. The Officer should have personal knowledge of the circumstances of the crime/s to be prevented and an understanding of The Code.
 - 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 Code.
- 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.

5. 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 data controller complying with a request to supply a copy of the data to the subject, only data pertaining to the individual should be copied, (all other personal data which may facilitate the identification of any other person should be concealed or erased). Under these circumstances an additional fee may be payable.
 - c) The data controller is entitled to refuse an individual request to view data under these provisions if insufficient or inaccurate information is provided, however every effort should be made to comply with subject access procedures and each request should be treated on its own merit.
 - d) In addition to the principles contained within the Data Protection legislation, the data controller should be satisfied that the data is:
 - i) Not currently and, as far as can be reasonably ascertained, not likely to become, part of a 'live' criminal investigation;
 - ii) Not currently and, as far as can be reasonably ascertained, not likely to become, relevant to civil proceedings;
 - iii) Not the subject of a complaint or dispute that has not been actioned;
 - iii) The original data and that the audit trail has been maintained;
 - iv) Not removed or copied without proper authority;
 - v) For individual disclosure only (i.e. to be disclosed to a named subject)

6. Process of Disclosure

- a) Verify the accuracy of the request.
- b) Replay the data to the requestee only, (or responsible person acting on behalf of the person making the request).
- c) The viewing should take place in a separate room and not in the control or monitoring area. Only data that is specific to the search request shall be shown.
- d) It must not be possible to identify any other individual from the information being shown, (any such information will be blanked-out, either by means of electronic screening or manual editing on the monitor screen).
- e) If a copy of the material is requested and there is no on-site means of editing out other personal data, then the material shall be sent to an editing house for processing prior to being sent to the requestee.

7. Media disclosure

- a) In the event of a request from the media for access to recorded material, the procedures outlined under 'secondary request to view data' shall be followed. If material is to be released the following procedures shall be adopted:
 - i) The release of the material must be accompanied by a signed release document that clearly states what the data will be used for and sets out the limits on its use.

- ii) The release form shall state that the receiver must process the data in a manner prescribed by the data controller, e.g. specific identities/data that must not be revealed.
- iii) It shall require that proof of any editing must be passed back to the data controller, either for approval or final consent, prior to its intended use by the media (protecting the position of the data controller who would be responsible for any infringement of Data Protection legislation and The Code).
- iv) The release form shall be considered a contract and signed by both parties.

8. Principles

In adopting this national standard for the release of data to third parties, it is intended, as far as reasonably practicable, to safeguard the individual's rights to privacy and to give effect to the following principles:

- a) Recorded material shall be processed lawfully and fairly and used only for the purposes defined in The Code;
- b) Access to recorded material shall only take place in accordance with this Standard and The Code;
- c) The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

WARNING

RESTRICTED

ACCESS AREA

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

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

Confidentiality Clause:

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

Appendix C Declaration of Confidentiality

The Herefordshire CCTV System Declaration of Confidentiality

I,, am retained by to perform the duty of CCTV Control Room Operator on behalf of The Partnership. I have received a copy of The Code in respect of the operation and management of The System.

I hereby declare that:

I am fully conversant with the content of The Code and understand that all duties which I undertake in connection with The System must not contravene any part of The Code, 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, 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 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 System).

In appending my signature to this declaration, I agree to abide by The Code 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.

I further acknowledge that I have been informed and clearly understand that the communication, either verbally or in writing, to any unauthorised person(s) of any information acquired as a result of my employment with may be an offence against the Official Secrets Act of 1911, Section 2, as amended by the Official Secrets Act of 1989.

Signed: Print Name:

Witness: Position:

Dated this day of (month) 20.....

Appendix D Inspector's Declaration of Confidentiality

The Herefordshire CCTV System Inspector's Declaration of Confidentiality

I, am a voluntary Inspector of the Herefordshire CCTV System with a responsibility to monitor the operation of The System and adherence to The Code. 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 with the content of The Code. I undertake to inform the System Manager of any apparent contraventions of The Code 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 System or the content of The Code, 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 System, 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 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 this day of (month) 20.....

Appendix E Subject Access Request Form

SUBJECT ACCESS REQUEST FORM HEREFORDSHIRE CCTV SURVEILLANCE SYSTEM DATA PROTECTION ACT, 1998

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

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

Your Rights

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

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

Herefordshire Council's Rights

Herefordshire Council may deny access to information where the Act allows. The main exemptions in relation to information held on the CCTV System are where the information may be held for:

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

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

Fee

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

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

Section 1 Asks you to give information about yourself that will help the Council to confirm your identity. Herefordshire Council has a duty to ensure that information it holds is secure and it must be satisfied that you are who you say you are.

Section 2 Asks you to provide evidence of your identity by producing TWO official documents (which between them clearly show your name, date of birth and current address) together with a recent full face photograph of you.

Section 3 Asks you to confirm whether you will accept just viewing the information, or if you want a copy of the information.

Section 4 You must sign the declaration

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

The Commissioning Officer (CCTV), PO Box 4, Plough Lane, Hereford HR4 0XH
or take it to any main Info in Herefordshire Office in this District.
(Receptionist – please complete 'Official Use' Section on page 5.)

**If you have any queries regarding this form, or your application, please ring the
Commissioning Officer (CCTV) on Tel No. 01432 261713**

HEREFORDSHIRE CCTV SURVEILLANCE SYSTEM DATA PROTECTION ACT 1998

SECTION 1 About Yourself

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

PLEASE USE BLOCK LETTERS

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

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

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

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

SECTION 2 Proof of Identity

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

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

Also a recent, full face photograph of yourself.

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

SECTION 3 Supply of Information

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

(a) View the information and receive a permanent copy

YES / NO

(b) Only view the information

YES / NO

NOW – please complete Section 4 and then check the ‘CHECK’ box (on page 5) before returning the form.

SECTION 4 Declaration

DECLARATION (to be signed by the applicant)

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

Signed by

Date

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

SECTION 5**To Help us Find the Information**

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

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

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

Were you: (tick box below)

A person reporting an offence or incident

A witness to an offence or incident

A victim of an offence

A person accused or convicted of an offence

Other – please explain

Date(s) and time(s) of incident

Place incident happened

Brief details of incident

Before returning this form:

- Have you completed ALL Sections in this form?

Please check:

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

Further Information:

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

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

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

OFFICIAL USE ONLY

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

Application checked and legible?	<input type="checkbox"/>	Date Application Received	<input type="text"/>
Identification documents checked?	<input type="checkbox"/>	Fee Paid	<input type="text"/>
Details of 2 Documents (see page 3)	<input type="text"/>	Method of Payment	<input type="text"/>
		Receipt No.	<input type="text"/>
		Documents Returned?	<input type="text"/>

Member of Staff completing this Section:

Name	<input type="text"/>	Location	<input type="text"/>
Signature	<input type="text"/>	Date	<input type="text"/>

Appendix F Maps of Herefordshire Camera Locations

Hereford

Ledbury

Leominster

Ross-on-Wye

Appendix G Regulation of Investigatory Powers Act 2000 Guiding Principles

Introduction

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

The guidance contained in this Code of Practice serves to explain and highlight the legislation to be considered. A more detailed section will be included in the Model Procedural Manual to assist users in the application of the requirements

Background

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

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

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

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

"Covert surveillance" defined

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

Part II - Surveillance types

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

“Intrusive” surveillance

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

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

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

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

Our CCTV cameras are deemed incapable of providing this level of detail so as to be considered “intrusive” for the purposes of the act. Current interpretations re sustained gathering of images of persons in a car in a car park dealing in drugs; being able to see clearly inside the car, would not be considered “intrusive” under the act.

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

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

“Directed” surveillance

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

The act says:

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

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

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

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

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

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

Authorisations

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

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

A Local Authority (within the meaning of section 1 of the Local Government Act 1999). The prescribed office as a minimum level of authority is:

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

Police Forces - A police force maintained under section 2 of the Police Act 1996 (police forces in England and Wales). The prescribed level is a Superintendent; for urgent cases an Inspector.

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

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

The 'authority' must indicate the reasons and should fall within one of the following categories:-
An authorisation is necessary on grounds falling within this subsection if it is necessary-

- (a) *in the interests of national security;*
- (b) *for the purpose of preventing or detecting crime or of preventing disorder;*
- (c) *in the interests of the economic well-being of the United Kingdom;*
- (d) *in the interests of public safety;*
- (e) *for the purpose of protecting public health;*
- (f) *for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or*
- (g) *for any purpose (not falling within paragraphs (a) to (f)) which is specified for the purposes of this subsection by an order made by the Secretary of State.*

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

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

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

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

Policing examples:

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

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

Supt Authorisation – non-urgent request

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

No authorisation required

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

For access to all relevant information on this Act , including the Schedules and Statutory Instruments referred to in this guidance please visit:

www.homeoffice.gov.uk/ripa/ripact.htm

Appendix H Glossary

CCTV - Closed Circuit Television

The Herefordshire Council - The County of Herefordshire District Council

The Partnership - The County of Herefordshire District Council and West Mercia Police

The Police Station - Hereford Police Station

The Code - Code of Practice

The System – Closed Circuit Television systems belonging to the Herefordshire Council

Data Controller – The County of Herefordshire District Council

WORM – Write Once Read Many

RIPA – Regulation of Investigatory Powers Act 2000