

Exeter Community Safety Partnership

Exeter CCTV System Code of Practice

CCTV Enquiries

The Control Centre Manager

Devon County Council
County Hall
Topsham Road
Exeter EX2 4QW

Tel: 01392 382884

CCTV Enquiries

The Control Room Manager

Control Centre Manager
Environmental Health Services
Exeter City Council
Civic Centre
Paris St.
Exeter EX1 1RQ

Tel: 0845 351 1060

Acknowledgements

This Code of Practice has been based on *The CCTV User Group Model Code of Practice* which in turn was compiled using elements of *good practice* across the country and existing guidance notes including '*A Watching Brief*' published by the Local Government Information Unit in March 1996, the Information Commissioners CCTV Code of Practice based on the Data Protection Act 1998, and other recent legislation that affects the use of CCTV.

Revisions

Rev 2 14-Jan-02 agreed by Exeter CCTV Ethics Committee

Rev 3 11-Sep-06 agreed by Exeter CCTV Ethics Committee


Code of Practice in Respect of the Operation of The Exeter CCTV System

Agreed by
Devon County Council
Exeter City Council
Devon & Cornwall Constabulary

Certificate of Agreement


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

Signed for and on behalf of *Devon County Council*

Signature:  Dated: 14th January 2002

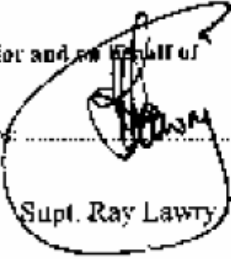
Name: Mr. Edward Chorlton Position: *County Environment Director*

Signed for and on behalf of *Exeter City Council*

Signature:  Dated: 14th January 2002

Name: Ms. Hazel Ball Position: *Community and Environment Director*

Signed for and on behalf of *Devon & Cornwall Constabulary*

Signature:  Dated: 14th January 2002

Name: Supt. Ray Lawry Position: *Exeter District Commander*

CONTENTS

1.	INTRODUCTION AND OBJECTIVES	6
1.1	Introduction	6
1.2	Definitions.....	6
1.3	Partnership statement in respect of The Human Rights Act 1998.....	6
1.4	Objectives of the System	7
2.	STATEMENT OF PURPOSE AND PRINCIPLES	8
2.1	Purpose.....	8
2.2	General Principles of Operation	8
2.3	Copyright	8
2.4	Cameras and Area Coverage	8
2.5	Monitoring and Recording Facilities.....	9
2.6	Human Resources.....	9
2.7	Processing and Handling of Recorded Material	9
2.8	Operators Instructions	9
2.9	Changes to the Code.....	9
3.	PRIVACY AND DATA PROTECTION	10
3.1	Public Concern.....	10
3.2	Data Protection Legislation	10
3.3	Request for information (subject access).....	11
3.4	Exemptions to the Provision of Information	11
4.	ACCOUNTABILITY AND PUBLIC INFORMATION	12
4.1	The Public	12
4.2	System Manager.....	12
4.3	Public Information	12
	Code of Practice	12
	Signs	12
5.	ASSESSMENT OF THE SYSTEM AND CODE OF PRACTICE	14
5.1	Evaluation	14
5.2	Monitoring	14
5.3	Audit	14
6.	HUMAN RESOURCES	15
6.1	Staffing of the Monitoring Room.....	15
6.2	Discipline	15
6.3	Declaration of Confidentiality	15
7.	CONTROL AND OPERATION OF CAMERAS	16
7.1	Guiding Principles	16
7.2	Operation of The System by the Police	16
7.3	Maintenance of the System.....	16
8.	SECURITY ARRANGEMENTS OF MONITORING ROOM	18
8.1	Security Arrangements.....	18
8.2	Public access and visits.....	18
8.3	Declaration of Confidentiality	18
9.	MANAGEMENT OF RECORDED MATERIAL	19
9.1	Guiding Principles	19
9.2	National standard for the release of data to a third party.....	19
9.3	Recorded Material – Retention	20
9.4	Register of recorded material	20
9.5	Release of recorded material.....	20
9.6	Prints of recorded material	20
A.1	KEY PERSONNEL AND RESPONSIBILITIES	21
A.2	LOCATION AND OWNERSHIP OF CAMERAS	22
A.3	NATIONAL STANDARD FOR THE RELEASE OF DATA TO THIRD PARTIES	23
A.4	EXAMPLE OF RESTRICTED ACCESS NOTICE	26
A.5	DECLARATION OF CONFIDENTIALITY	27
A.6	REGULATION OF INVESTIGATORY POWERS – GUIDING PRINCIPALS	28
A.7	SUBJECT ACCESS REQUEST FORM	29

1. Introduction and Objectives

1.1 Introduction

A Closed Circuit Television (CCTV) System has been introduced to Exeter. This System, known as the Exeter CCTV System, comprises a number of cameras installed at strategic locations. The cameras are fully operational and either fixed or with pan, tilt and zoom facilities. Most are colour but some are monochrome. The System is operated from two control centres within the city, some images being available in only one control room, whilst some are available for viewing in both locations.

The Exeter CCTV System has evolved from the formation of a partnership between Devon County Council, Exeter City Council and Devon and Cornwall Constabulary who all certify their acceptance of the requirements of this code, by way of a signature at the front of this document. Local business consortiums have also been closely consulted and involved with the establishment of this System.

The Exeter CCTV System has been notified to the Information Commissioner

1.2 Definitions

Data Controller	means Devon County Council, Exeter City Council and Devon and Cornwall Constabulary.
Owner	means Devon County Council and Exeter City Council
System Manager	means Control Centre Managers of Devon County Council and Exeter City Council

Details of key personnel, their responsibilities and contact points are shown at appendix A.1 to this Code.

Devon County Council and Exeter City Council are each responsible for managing their own control centres and monitoring, recording and maintaining their own cameras whilst operating under this common Code of Practice and liaising closely. Sharing of images and undertaking further third party monitoring will be at the discretion of the individual authority.

1.3 Partnership statement in respect of The Human Rights Act 1998

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. The partnership considers that the use of CCTV in Exeter is a necessary, proportionate and suitable tool to help reduce crime, reduce the fear of crime and improve public safety.

Section 163 of the Criminal Justice and Public Order Act 1994 creates the power for local authorities to provide closed circuit television coverage of any land within their area for the purposes of crime prevention or victim welfare. The Local Authorities and Police also consider it a necessary initiative towards their duty under the Crime and Disorder Act 1998.

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

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

The Codes of Practice and observance of the Operational Procedures contained in the manual shall ensure that evidence is secured, retained and made available as required so that there is absolute respect for everyone's right to a free trial.

1.4 Objectives of the System

The objectives of the Exeter CCTV System as determined by the Data Controller and which form the lawful basis for the processing of data are:-

- *To help reduce the fear of crime*
- *To help deter and detect crime and provide evidential material for court proceedings*
- *To assist in the overall management of Exeter City Centre*
- *To help deter and detect acts of anti-social behaviour*
- *To enhance community safety, assist in developing the economic well being of the Exeter area and encourage greater use of the City Centre*
- *To assist the Local Authorities in their enforcement and regulatory functions within the Exeter area*
- *To assist in Traffic Management, and encourage safer and more sustainable use of all modes of transport and provide travel information to the media and public*
- *To assist in supporting civil proceedings*
- *To monitor all modes of travel to enable improvement and better management of the public highway*

Within this broad outline, the Data Controller may draw up specific key objectives (which will be reviewed annually) based on local concerns.

2. Statement of Purpose and Principles

2.1 Purpose

The purpose of this document is to state how the owners and the managers, on behalf of the partnership as a whole intend to use the Exeter CCTV System, (hereafter referred to as 'The System') to meet the objectives and principles outlined in Section 1.

2.2 General Principles of Operation

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

The operation of the System will also recognise the need for formal authorisation of surveillance as required by the Regulation of Investigatory Powers Act 2000, in particular Part 2 of the Act, and the police force policy.

The System will be operated in accordance with the Data Protection Act 1998 at all times

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

The System will be operated with due regard to a general right to respect for his or her private and family life and their home.

The public interest in the operation of the System will be safeguarded by ensuring the security and integrity of operational procedures.

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

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

2.3 Copyright

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

2.4 Cameras and Area Coverage

This Code of Practice refers are to those areas within the responsibility of the operating partners.

Where mobile cameras are deployed, they will be remotely connected to the control centre and their operation will be similar to fixed camera installations

All cameras within the System will be positioned within an area suitably signed to alert of their presence.

Details of the location of all cameras will be made publicly available.

2.5 Monitoring and Recording Facilities

All cameras are connected to one or both of the System's control centres. All images captured by the System are recorded throughout every 24 hour period by the control centre designated for that purpose.

2.6 Human Resources

Staff will be suitably trained and authorised visitors will not have access to the monitoring room without an authorised member of staff being present.

2.7 Processing and Handling of Recorded Material

No recorded material, whether recorded digitally, in analogue format or as a hard copy video print, will be released from the control centre unless it is in accordance with this Code of Practice.

2.8 Operators Instructions

Each control centre shall produce its own procedures which shall comply with this Code of Practice.

2.9 Changes to the Code

Any major changes to the Code of Practice, will take place only after consultation with, and upon the agreement of the Partnership.

A minor change, (i.e. such as may be required for clarification and will not have such a significant impact) may be agreed between the System Managers and the Owners of the System.

3. Privacy and Data Protection

3.1 Public Concern

Although the majority of the public at large may have become accustomed to 'being watched', those who do express concern, do so mainly over matters pertaining to the processing of the information, (or data) i.e. what happens to the material that is obtained.

All personal data obtained by virtue of The System, shall be processed fairly and lawfully and, in particular, shall only be processed in the exercise of achieving the stated objectives of the System. In processing personal data a person's right to respect for his or her private and family life and their home will be respected.

The processing, storage and security of the data will be strictly in accordance with the requirements of the Data Protection Act 1998 and additional locally agreed procedures.

Cameras will not be used to look into private residential property, unless pursuing a suspect and this is considered to be in the interests of the private residents. 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.

3.2 Data Protection Legislation

The operation of The System has been notified to the Office of the Information Commissioner in accordance with current Data Protection legislation.

The 'data controller' for The System' is Devon County Council, Exeter City Council and Devon and Cornwall Constabulary and day to day responsibility for the data will be devolved to the System Managers.

All data will be processed in accordance with the principles of the Data Protection Act, 1998 which are in summarised form:

- All personal data will be processed fairly and lawfully.
- Personal data will be obtained only for the purposes specified.
- Personal data held will be adequate, relevant and not excessive in relation to the purpose for which the data is processed.
- Steps will be taken to ensure that personal data is accurate and where necessary, kept up to date.
- Personal data will be held for no longer than is necessary.
- Individuals will be allowed access to personal data, in accordance with individual's rights
- Procedures will be implemented to ensure security measures to prevent unauthorised or accidental access to, alteration, disclosure, or loss and destruction of, information.
- Information shall not be transferred outside the European Economic Area unless the rights of individuals are protected.

3.3 Request for information (subject access)

Any request from an individual for the disclosure of personal data which he / she believes is recorded by virtue of the System will be directed in the first instance to the System Manager.

The principles of the Data Protection Act 1998 shall be followed in respect of every request. Individuals whose image is captured on CCTV, but who are not the target of the surveillance are not entitled to make an access request.

If the request cannot be complied with without identifying another individual, permission from that individual must be obtained unless it is reasonable in all the circumstances to comply with the request without the consent of that individual.

Any person making a request must be able to satisfactorily prove their identity and provide sufficient information to enable the data to be located.

3.4 Exemptions to the Provision of Information

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

Personal data processed for any of the following purposes -

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

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

4. Accountability and Public Information

4.1 The Public

For reasons of security and confidentiality, access to the CCTV monitoring room is restricted in accordance with this Code of Practice.

A member of the public wishing to register a complaint with regard to any aspect of The System may do so by contacting the System Manager's office. All complaints shall be dealt with in accordance with the Devon County Council or Exeter City Council complaints procedure (as appropriate), a copy of which may be obtained from Devon County Council or Exeter City Council offices. Any performance issues identified will be considered under the relevant organisations disciplinary procedures to which all employees, including CCTV personnel are subject.

4.2 System Manager

The nominated manager(s) named at appendix A.1 will have day-to-day responsibility for the System as a whole.

The System Managers will provide an annual report on the operation of the System to designated representatives of the Exeter Community Safety Partnership, including the opportunity to review this Code of Practice.

The System will be subject to the usual Local Government audit arrangements.

The appropriate System Manager will ensure that every complaint is acknowledged within ten working days which will include advice to the complainant of the enquiry procedure to be undertaken. A record of all complaints will be kept and routinely reported to the Partnership.

4.3 Public Information

Code of Practice

A copy of this Code of Practice shall be published on Devon County Council and Exeter City Council web sites, and a copy will be made available to anyone on request. Additional copies will be lodged at public libraries, Heavitree Road police station, County Hall and Civic Centre reception offices.

Leaflets detailing the operation of the CCTV system will also be made publicly available.

Signs

Signs (similar to that shown below) will be placed in the locality of the cameras and at main entrance points to the relevant areas. The signs will indicate:

- The presence of CCTV monitoring;
- The 'ownership' of the System;
- Contact telephone number for the System.



5. Assessment of the System and Code of Practice

5.1 Evaluation

The System will, periodically, be evaluated to establish whether the purposes of the System are being complied with and whether objectives are being achieved.

5.2 Monitoring

The System Manager will accept day to day responsibility for the monitoring and operation of the System and the implementation of this Code of Practice.

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

5.3 Audit

There will be regular audits of the operation of the System and the compliance with this Code of Practice. Audits, which may be in the form of irregular spot checks, will include examination of the monitoring room records, media histories and the content of recorded material.

6. Human Resources

6.1 Staffing of the Monitoring Room

Control centre operators will not be permitted to use the CCTV system until they have received suitable basic training and are familiar with this code of practice. They will also receive further training and assessment to the level required by the Security Industry Authority (PSS) standard, and where required, be licensed by the SIA.

Where a control centre requires operators to be licensed, in accordance with the law, no staff may operate cameras subject to the legislation without a licence.

Every person involved in the management and operation of the System will be personally issued with a copy of the Code of Practice. They will be required to sign confirming that they fully understand their obligations to adhere to these documents and that any breach is likely to be considered a disciplinary offence. They will be fully conversant with the contents of the code and appropriate procedures, which may be updated from time to time, and with which he / she will be expected to comply.

Arrangements may be made for a police liaison officer to be present in the monitoring room at certain times, or indeed at all times, subject to locally agreed protocols. Any such person must also be conversant and comply with this Code of Practice and associated procedures.

6.2 Discipline

Every individual with any responsibility under the terms of this Code of Practice and who has any involvement with The System to which they refer, will be subject to the Employing Authority's disciplinary code. Any breach of this Code of Practice or of any aspect of confidentiality will be dealt with in accordance with the relevant disciplinary procedure.

The System Manager will accept primary responsibility for ensuring there is no breach of security and that the Code of Practice is complied with. He/she has day to day responsibility for the management of the room and for ensuring compliance with the Code of Practice and procedures.

6.3 Declaration of Confidentiality

Every individual with any responsibility under the terms of this Code of Practice and who has any involvement with The System to which they refer, will be required to sign a declaration of confidentiality. (See example at appendix A.4, see also Section 8 concerning access to the monitoring room by others).

7. Control and Operation of Cameras

7.1 Guiding Principles

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

Cameras will not be used to look into private residential property, unless pursuing a suspect and this is considered to be in the interests of the public.

Camera operators will be mindful of exercising prejudices, which may lead to complaints of the System being used for purposes other than those for which it is intended. The operators may be required to justify their interest in, or recording of, any particular individual, group of individuals or property at any time by virtue of the audit of the System or by the System Manager.

7.2 Operation of The System by the Police

Under extreme circumstances the Police may make a request to assume direction of The System to which this Code of Practice applies. Only requests made on the written authority of a police officer of Superintendent rank or above will be considered. Any such request will only be accommodated on the personal written authority of the most senior representative of the Owners, or designated deputy of equal standing.

In the event of such a request being permitted, the monitoring room will continue to be staffed, and equipment operated by, only those personnel who are authorised to do so, and who fall within the terms of Sections 6 and 7 of this Code, who will then operate under the direction of the police officer designated in the written authority.

In very extreme circumstances a request may be made for the Police to take total control of The System in its entirety, including the staffing of the monitoring room and personal control of all associated equipment, to the exclusion of all representatives of the Owners. Any such request must be made to The System Manager in the first instance, who will consult personally with the most senior officer of The Owners (or designated deputy). A request for total exclusive control must be made in writing by a police officer of the rank of Assistant Chief Constable or above.

7.3 Maintenance of the System

To ensure compliance with the Information Commissioners Code of Practice and that images recorded continue to be of appropriate evidential quality The Exeter CCTV System shall be maintained under a maintenance agreement.

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.

The maintenance will also include regular periodic overhaul of all the equipment and replacement of equipment which is reaching the end of its serviceable life.

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.

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.

It is the responsibility of the System Manager to ensure appropriate records are maintained in respect of the functioning of the cameras and the response of the maintenance organisation.

8. Security Arrangements of Monitoring Room

8.1 Security Arrangements

The monitoring room will have a physical means of security and authorised personnel will normally be present at all times when the equipment is in use. Only trained and authorised personnel will operate any of the equipment located within the CCTV monitoring room, (or equipment associated with the CCTV System).

8.2 Public access and visits

Public access to the monitoring and recording facility will be controlled at the discretion of the System Manager, and visitors will be supervised at all times. Any such visits will be conducted and recorded .

8.3 Declaration of Confidentiality

All visitors to the CCTV monitoring room, including auditors, will be required to sign the visitors book and a declaration of confidentiality:

'In signing this visitors book I, a visitor to the Exeter CCTV System monitoring room acknowledge that the precise location of the CCTV monitoring room and personal details of those operating the System are confidential and must remain so. I further agree not to divulge any information obtained, overheard or seen during my visit.'

Staff who regularly access the Control Room will sign a separate statement of this declaration of confidentiality which will be kept on file.

9. Management of Recorded Material

9.1 Guiding Principles

For the purposes of this Code 'recorded material' means any material recorded by, or as the result of, technical equipment which forms part of The System, but specifically includes images recorded digitally, or on videotape or by way of video copying, including video prints.

Every video or digital recording obtained by using The System has the potential of containing material that may need to be admitted in evidence at some point during the period of its retention.

Members of the community must have total confidence that information recorded about their ordinary every day activities by virtue of The System, will be treated with due regard to their individual right to respect for their private and family life.

It is therefore of the utmost importance that irrespective of the means or format (e.g. paper copy, video tape, digital tape, CD, or any form of electronic processing and storage) of the images obtained from the System, they are treated strictly in accordance with this Code of Practice from the moment they are received by the monitoring room until final destruction. Every movement and usage will be meticulously recorded.

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

Recorded material will not be copied, sold, otherwise released or used for commercial purposes or for the provision of entertainment or otherwise made available for any use incompatible with this Code of Practice.

Information will be made available for traffic and transport monitoring, management and information purposes, and those cameras which will be permanently broadcast on the Internet are identified in the Appendix .

9.2 National standard for the release of data to a third party

Every request for the release of personal data generated by this CCTV System will be channelled through the System Manager. The System Manager will ensure the principles contained within Appendix A.3 to this Code of Practice are followed at all times.

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

- Recorded material shall be processed lawfully and fairly, and used only for the purposes defined in this Code of Practice;
- Access to recorded material will only take place in accordance with the standards outlined in appendix A.3 and this Code of Practice;

Members of the police service or other agency having a statutory authority to investigate and / or prosecute offences may, subject to compliance with appendix A.3, 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. 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.3.

It may be beneficial to make use of 'real' video footage for the training and education of those involved in the operation and management of CCTV Systems, and for those involved in the investigation, prevention and detection of crime. Any material recorded by virtue of this CCTV System will only be used for such bona fide training and education purposes.

9.3 Recorded Material – Retention

Recorded material will be retained for a period of one calendar month. Before reuse or destruction, recorded material will be magnetically erased in full accordance with the manufacturer's requirements, wherever possible. Digital recording will be set to overwrite automatically.

At the conclusion of their life recorded material used within the CCTV System will be destroyed.

9.4 Register of recorded material

Each discrete item of recorded material (tape, CD, DVD etc) will be registered and monitored from the time it is produced, until it is destroyed, whilst it is within the control centres. Records will be retained for at least three years.

9.5 Release of recorded material

If recorded material is released in accordance with this code, a record must be kept which identifies the basis for that release, and to whom. Records will be retained for at least three years.

9.6 Prints of recorded material

Prints, subject to Data Protection, will be treated in the same way as other recorded information identified above. They will not be released outside the control centre except as permitted by this code, and any release will be recorded.

Where prints, which contain personal data, are taken for use within the control centre, they should not be kept for longer than can be reasonably justified, and should be regularly reviewed.

Prints that are no longer required should be securely destroyed.

A.1 Key Personnel and Responsibilities

System Owners

The Exeter CCTV System is jointly owned by Devon County Council and Exeter City Council, both of whom bear the responsibility for maintaining the System. The initial capital funding of the System has come from a number of sources including Central Government, the Local Authorities and Local Businesses.

Devon County Council
County Hall
Topsham Road
Exeter EX2 4QW

Tel: 01392 382884

Exeter City Council
Civic Centre
Paris Street
Exeter EX1 1JN

Tel: 01392 277888

Responsibilities:

- Ensure the provision and maintenance of all equipment forming part of the Exeter CCTV System in accordance with contractual arrangements, which the owners may from time to time enter into.
- Maintain close liaison with the control room manager.
- Ensure the interests of the owners and other organisations are upheld in accordance with the terms of this Code of Practice.
- Agree to any proposed alterations and additions to the System, this Code of Practice and / or the Procedural Manual.

Operational Management

The Control Centre Manager
Devon County Council
County Hall
Topsham Road
Exeter EX2 4QW

Tel: 01392 382884

The Control Room Manager
Control Centre Manager
Environmental Health Services
Exeter City Council
Civic Centre
Paris St.
Exeter EX1 1RQ

Tel: 0845 351 1060

Responsibilities:

- The Control Room Manager is the 'manager' of the Exeter CCTV System
- He has delegated authority for day to day management on behalf of the 'data controller'.
- To maintain day to day management of the System and staff;
- To accept overall responsibility for the System and for ensuring that this Code of Practice is complied with;
- To maintain direct liaison with the owners of the System and operating partners.

A.2 Location and Ownership of Cameras

The latest list of cameras and ownership are available on the Devon County Council and Exeter City Council websites:

www.devon.gov.uk/cctv/

www.exeter.gov.uk

A.3 National Standard for the release of data to third parties

A.3.1 Introduction

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

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

After considerable research and consultation, the nationally recommended standard of The CCTV User Group has been adopted by the System owners.

A.3.2 General Policy

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

A.3.3 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;
 - 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) Claimants in civil proceedings
 - v) Accused persons or defendants in criminal proceedings
 - vi) Other agencies, (as agreed by the Data Controller and notified to the Information Commissioner) 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) Where requests fall outside the terms of disclosure and Subject Access legislation, 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.

A.3.4 Secondary Request To View Data

- a) A 'secondary' request for access to data may be defined as any request being made which does not fall into the category of a primary request. Before complying with a secondary request, the data controller shall ensure that:
 - i) The request does not contravene, and that compliance with the request would not breach, current relevant legislation, (e.g. Data Protection Act 1998, Human Rights Act 1998, section 163 Criminal Justice and Public Order Act 1994, etc.);
 - ii) Any legislative requirements have been complied with, (e.g. the requirements of the Data Protection Act 1998);
 - iii) Due regard has been taken of any known case law (current or past) which may be relevant, (e.g. R v Brentwood BC ex p. Peck) and
 - iv) The request would pass a test of 'disclosure in the public interest'⁽¹⁾.
- b) If, in compliance with a secondary request to view data, a decision is taken to release material to a third party, the following safeguards shall be put in place before surrendering the material:
 - i) In respect of material to be released under the auspices of 'crime prevention', written agreement to the release of the material should be obtained from a police officer, not below the rank of Inspector. The officer should have personal knowledge of the circumstances of the crime/s to be prevented and an understanding of the CCTV System Code of Practice⁽²⁾.
 - ii) If the material is to be released under the auspices of 'public well being, health or safety', written agreement to the release of material should be obtained from a senior officer within the Local Authority. The officer should have personal knowledge of the potential benefit to be derived from releasing the material and an understanding of the CCTV System Code of Practice.
- c) Recorded material may be used for bona fide training purposes such as police or staff training. Under no circumstances will recorded material be released for commercial sale of material for training or entertainment purposes.

A.3.5 Individual Subject Access under Data Protection legislation

- 1) Under the terms of Data Protection legislation, individual access to personal data, of which that individual is the data subject, must be permitted providing:
 - i) The request is made in writing;
 - ii) A specified fee is paid for each individual search;
 - iii) The data controller is supplied with sufficient information to satisfy him or her self as to the identity of the person making the request;
 - iv) The person making the request provides sufficient and accurate information about the time, date and place to enable the data controller to locate the information which that person seeks, (it is recognised that a person making a request is unlikely to know the precise time. Under those circumstances it is suggested that within one hour of accuracy would be a reasonable requirement);
 - v) The person making the request is only shown information relevant to that particular search and which contains personal data of her or him self only, unless all other individuals who may be identified from the same information have consented to the disclosure;

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

A.3.6 Process of Disclosure:

- a) Verify the accuracy of the request.
- b) Replay the data to the requestee only, (or responsible person acting on behalf of the person making the request).
- c) The viewing should take place in a separate room and not in the control or monitoring area. Only data which is specific to the search request shall be shown.
- d) It must not be possible to identify any other individual from the information being shown, (any such information will be blanked-out, either by means of electronic screening or manual editing on the monitor screen).
 - 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.

A.3.7 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, and indemnifies the partnership against any breaches of the legislation.
 - ii) The release form shall state that the receiver must process the data in a manner prescribed by the data controller, e.g. specific identities/data that must not be revealed.
 - iii) It shall require that proof of any editing must be passed back to the data controller, either for approval or final consent, prior to its intended use by the media (protecting the position of the data controller who would be responsible for any infringement of Data Protection legislation and the System's Code of Practice).
 - iv) The release form shall be considered a contract and signed by both parties.

A.4 Example of Restricted Access Notice

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 signing this visitors book I, a visitor to the Exeter CCTV System monitoring room acknowledge that the precise location of the CCTV monitoring room and personal details of those operating the System are confidential and must remain so. I further agree not to divulge any information obtained, overheard or seen during my visit.'

A.5 Declaration of Confidentiality

The Exeter CCTV System

I,, am employed by Devon County Council to undertake monitoring of the Exeter CCTV System. I have received a copy of the Code of Practice in respect of the operation and management of that CCTV System.

I hereby declare that:

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

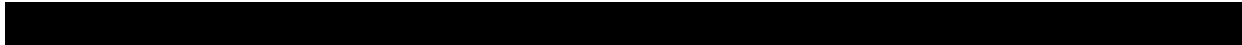
I understand that it is a condition of my employment that I do not disclose or divulge to any individual, firm, company, authority, agency or other organisation, any information which I may have acquired in the course of, or for the purposes of, my position in connection with the Exeter CCTV System,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

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

Signed: Print Name:

Witness: Position:

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



A.6 Regulation of Investigatory Powers – Guiding Principals

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

The Regulation of Investigatory Powers Act 2000 relates to surveillance by the Police and other agencies and deals in part with the use of directed covert surveillance. Section 26 of this act sets out what is Directed Surveillance. It defines this type of surveillance as:-

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

- (a) for the purposes of a specific investigation or a specific operation;*
- (b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and*
- (c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance*

The impact for staff in the Police control rooms and CCTV monitoring centres, is that there might be cause to monitor for some time, a person or premises using the cameras. In most cases, this will fall into sub section **c** above, i.e. it will be an immediate response to events or circumstances. In this case, it would not require authorisation unless it were to continue for some time.

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

Slow time requests are authorised by a Superintendent or above.

If an authority is required immediately, an Inspector may do so. The forms in both cases must indicate the reason and should fall within one of the following categories:-

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

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

In cases where there is doubt as to whether an authorisation is required or not, it may be prudent to obtain the necessary authority verbally and then in writing by way of the forms. Any authority given should be recorded appropriately for later reference. This should include the name of the officer authorising.

Forms should be available at each CCTV monitoring centre and are included in the procedural manual.

A.7 Subject Access Request Form

Attached to this document is a copy of the standard Subject Access Form that has been designed for use by any individual that wishes to exercise their right to obtain information held on CCTV about themselves.