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, as far as is reasonably practicable, will be complied with by all who are involved in the management and operation of the System.

Signed for and on behalf of *Devon County Council*

Signature: .....…….....…… Dated the ..... day of ..... 20…

Name: …….. Position held: ……

Signed for and on behalf of *Exeter City Council*

Signature: .....…….....……..... Dated the ..... day of ..... 20…

Name: ……..…. Position held: ……

Signed for and on behalf of *Exeter District Commander, Devon & Cornwall Constabulary*

Signature: .....…….....……..... Dated the ..... day of ..... 20…

Name: ……..…. Position held: ……

CONTENTS

1. Introduction and Objectives

1.1 Introduction

A Closed Circuit Television (CCTV) System was introduced in Exeter in 2003. The System, known as the 'Exeter CCTV System' comprises a number of cameras installed at strategic locations. The majority of the cameras are fully operational with pan, tilt and zoom facilities. Others are fixed cameras, images from which are presented in the same room. The System is operated from two control centres within the City and are both covered in general by this Code of Practice.

The Exeter CCTV System has evolved from the original formation of the partnership between Devon County Council, Exeter City Council and Devon and Cornwall Constabulary and this review recognises the changes in legislation and operation of the two control centres.

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 Devon County Council and Exeter City Council Control Room Managers.

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

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.

This assessment is evidenced by an agreed 'operational requirement' and as a result of a public crime survey. 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*
- *The help deter and detect crime and provide evidential material for court proceedings*
- *To assist in the overall management of Exeter City Centre*
- *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.

1.5 Procedural Manual

This Code of Practice (hereafter referred to as 'the Code') is supplemented by a separate 'Procedural Manual' which may be specific to each control centre. The Manual is not a public document but offers instructions on all aspects of the day to day operation of the System and Control Centre procedures. To ensure the purpose and principles (see Section 2) of the CCTV System are realised, the Procedural Manual is based and expands upon the contents of this Code of Practice.

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 the principle that everyone has the right to respect for his or her private and family life and their home. Article Eight of the European Convention on Human Rights defines the guiding principle: *"Everyone has the right to respect for his private and family life, his home and his correspondence."* This is subject to the exceptions set out under Article 8(2),
"*There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

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

The areas covered by CCTV to which this Code of Practice refers are public areas within the responsibility of the operating partners and cover Exeter and its environs.

From time to time transportable or mobile cameras may be temporarily sited within the area. The use of such cameras, and the data produced by virtue of their use, will always accord with the objectives of the CCTV System and be governed by this Code of Practice and any procedures ancillary to it.

Some of the cameras offer full colour, pan tilt and zoom (PTZ) capability, some of which may automatically switch to monochrome in low light conditions.

None of the cameras forming part of the System will be installed in a covert manner. Some cameras may be enclosed within 'All weather domes' for aesthetic or operational reasons but appropriate signs will identify the presence of all cameras.

Details of the location of all fixed cameras are attached at Appendix A.2 to these Codes.

2.5 Monitoring and Recording Facilities

Two staffed monitoring rooms are located in Exeter. The CCTV equipment has the capability of recording all cameras simultaneously throughout every 24 hour period

Additional monitoring equipment may be located in the City Centre. Each camera will be primarily recorded at only one location.

CCTV operators are able to record images from selected cameras in real-time, produce copies of recorded images, replay or copy any recorded data at their discretion and in accordance with the Code of Practice. All viewing and recording equipment shall only be operated by trained and authorised users.

2.6 Human Resources

Unauthorised persons will not have access to the monitoring room

The monitoring room shall be staffed by specially selected and trained operators who will be subject to Non Police Personnel Vetting.

All operators shall receive training relevant to their role in the requirements of the Human Rights Act 1998, Data Protection Act 1998, Regulation of Investigatory Powers Act 2000 and the Codes of Practice and Procedures. Further training will be provided as necessary.

2.7 Processing and Handling of Recorded Material

All recorded material will be processed and handled strictly in accordance with this Code of Practice and the Procedural Manual.

2.8 Operators Instructions

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

2.9 Changes to the Code or the Procedural Manual

Any major changes to either the Code of Practice or the Procedural Manual, 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 Manager 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', concern has been expressed in relation 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 Manager.

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 Policy Support Officer.

The principles of the Data Protection Act 1998 shall be followed in respect of every 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. The appropriate 'Subject Access' request form is included in Appendix A.7.

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 named at appendix A.1 will have day-to-day responsibility for the System as a whole.

The System Manager will provide routine reports on the operation of the System to designated representatives of the Exeter Community Safety Partnership.

Formal consultation will take place between the Partnership with regard to all aspects, including this Code of Practice and the Procedural Manual.

The 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.

Statistical and other relevant information, including any complaints made, will be included in the Annual Reports of the Partnership, which will be made publicly available.

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 to County Hall and Civic Centre reception offices.

Signs

Signs (as 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 independently evaluated to establish whether the purposes of the System are being complied with and whether objectives are being achieved. The format of the evaluation shall comply with that laid down by current Good Practice and be based on assessment of The Inputs, The Outputs, The Process and the Impact of the scheme covering the following:

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

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

It is intended that evaluations of the system should take place at least every five years.

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

Audits by regulatory bodies, which may be in the form of irregular spot checks, will include examination of the monitoring room records, video tape histories and the content of recorded material.

6. Human Resources

6.1 Staffing of the Monitoring Room

The CCTV Monitoring Room will be staffed in accordance with the Council's procedures Only Authorised personnel who will have been properly trained in its use will operate equipment associated with The System.

Every person involved in the management and operation of the System will have ready access to a copy of both the Code of Practice and the Procedural Manual and any breach is likely to be considered a disciplinary offence. .

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 Procedural Manual.

All personnel involved with the System shall receive training from time to time in respect of all legislation appropriate to their role.

6.2 Discipline

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 Procedural Manual.

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.

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.

Use of the cameras will accord with the purposes and key objectives of the System and shall be in compliance with this Code of Practice and Procedural Manual.

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.

The operators may be required to justify their interest in, or recording of, any particular individual, group of individuals or property at any time by virtue of the audit of the System or by the System Manager.

7.2 Primary Control

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

7.3 Secondary Control

Use of additional control and monitoring facilities will be administered and recorded in full accordance with this Code of Practice and the Procedural Manual and does not diminish in any way the obligations imposed on any of the persons involved to comply with all current legislative requirements.

7.4 Operation of the System by the Police

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 authority of the System Manager or designated deputy.

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 certain operational 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. Any such request must be made to the System Manager in the first instance, who may consult with the most senior officer of The Owners (or designated deputy). In extreme circumstances a request for total exclusive control of the System may be made in writing by a police officer of the rank of Assistant Chief Constable or above. Such a request would be considered by the highest level of management available at the time.

7.5 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 in accordance with the requirements of the Procedural Manual 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 in accordance with the Procedural Manual.

Visits by 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 auditors will visit at any one time. 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

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, including still image prints.

Every 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 its life span.

Members of the community may 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.

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

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 Appendix A.2.

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 Policy Support Unit. 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 in accordance with the Procedural Manual by the holder of the data.

If material is to be shown to witnesses, for the purpose of obtaining identification evidence, it must be shown in accordance with Appendix A.3 and the Procedural Manual.

It may be beneficial to make use of 'real' images 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 Images – Retention

Digital images will be overwritten after a period of one calendar month.

9.4 Recording Policy

Subject to the equipment functioning correctly, images from every camera will be recorded throughout every 24 hour period through digital multiplexers onto computer disk. The number of images through each multiplexer will be such that the time between successive frames once played back in time lapse mode shall not exceed 2 seconds.

9.5 Evidential Tapes

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

10. Image Prints

An Image print is a hard copy of an image held on computer disc and falls within the definition of 'data'.

The originator of a still imapge print is responsible for enuring that its capture and use use complies with current regulations and that the print is managed in accordance with the Procedural Manual.

Image prints contain data and will therefore only be released under the terms of Appendix A.3 to this Code of Practice, 'Release of data to third parties'. If prints are released to the media, (in compliance with Appendix A.3), in an effort to identify alleged offenders or potential witnesses, full details will be recorded in accordance with the relevant Procedural Manual.

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 came from a number of sources including Central Government and the Local Authorities.

Devon County Council **Tel: 01392 382884**
County Hall
Topsham Road
Exeter EX2 4QW

Exeter City Council **Tel: 01392 277888**
Civic Centre
Paris Street
Exeter EX1 1JN

Responsibilities:

- To 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.
- 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 Room Manager **Tel: 01392 382884**
Devon County Council
County Hall
Topsham Road
Exeter EX2 4QW

The Control Centre Manager **Tel: 0845 3511060**
Environmental Health Services
Exeter City Council
Civic Centre
Paris St.
Exeter EX1 1RQ

Responsibilities*:*

- The Control Room Manager's act jointly as 'manager' of the Exeter CCTV System
- They have 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

No	Location	Owner*
30	Sainsburys, Alphington cross	Devon County Council
38	Central Station platform 2	Devon County Council
41	Bus Station car park	Devon County Council
4	Countesswear Roundabout	Devon County Council
16	Fore Street, Heavitree	Devon County Council
1	Exe bridge	Devon County Council
40	Paris Street Roundabout	Devon County Council
8	Sidwell Street / St Annes Roundabout	Devon County Council

	2 Southgate Junction (The Acorn)	Devon County Council
	47 Alphinbrook Road / Church Road	Devon County Council
	46 Devon Hotel Roundabout	Devon County Council
	3 Marsh Barton Road / Alphington Road	Devon County Council
	42 Digby Park & Ride	Devon County Council
	31 Honiton Road Park & Ride	Devon County Council
	34 Matford Park & Ride	Devon County Council
	29 Sowton Park & Ride	Devon County Council
	45 Granada Roundabout	Devon County Council
#	6 M5 Jct 30, Sandygate East	Devon County Council
#	5 M5 Jct 30, Sandygate West	Devon County Council
	44 Moor Lane Roundabout	Devon County Council
	39 St Davids Station	Devon County Council
	10 Cowick Street	Devon County Council
	33 Topsham Road / Burnthouse Lane	Devon County Council

Bedford Street	Exeter City Council
Bradninch Hall	Exeter City Council
Broadgate	Exeter City Council
Bus Station Car Park	Exeter City Council
Cath/Quay Car Park	Exeter City Council
Cathedral Green	Exeter City Council
Cathedral St Petrocks & Bollard	Exeter City Council
Civic Centre & Southernhay	Exeter City Council
Civic Centre Car Cark	Exeter City Council
Civic Centre Mount	Exeter City Council
Civic Centre Paris Street	Exeter City Council
Civic Centre Rear Entrance	Exeter City Council
Dixs Field	Exeter City Council
Dixs Help Point	Exeter City Council
Fairpark Car Park	Exeter City Council
Fore Street	Exeter City Council
Gandy Street	Exeter City Council
George Street Car Park	Exeter City Council
Guildhall Car Park	Exeter City Council
High Street / Paris Street	Exeter City Council
King William Street Car Park	Exeter City Council
Longbrook Street	Exeter City Council
Magdalen Street Car Park	Exeter City Council
Market Street	Exeter City Council
Mary Aches Car Park	Exeter City Council
Mobile response camera (3)	Exeter City Council
Matford Park & Ride	Exeter City Council
Paul Street	Exeter City Council
Quayside	Exeter City Council
Queen Street	Exeter City Council
Queen Street/ Northernhay	Exeter City Council
Rennes House	Exeter City Council
Richmond Road	Exeter City Council
Sidwell Street	Exeter City Council
Smythen Street	Exeter City Council
South Street	Exeter City Council
South Street /Coombe Street	Exeter City Council
South Street Carfax	Exeter City Council
South Street/ Wetherspoons	Exeter City Council

Southernhay	Exeter City Council
St Thomas Park	Exeter City Council
West Street	Exeter City Council
York Road	Exeter City Council

* This column denotes the Authority responsible for the maintenance costs of each camera.
# denotes camera displaying images on Devon County Council website

A3 National Standard for the release of data to third parties

A.3.1 Introduction

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.

The recommended standard of the national CCTV User Group forms the basis of the Code 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 their 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[(1)].

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