DEVIZES DEVELOPMENT PARTNERSHIP

Business, community and local government, working in partnership for Devizes

Code of Practice
for the Operation of Closed Circuit Television
Devizes Town Centre

In partnership with

Devizes Chamber of Commerce
Devizes Community Area Planning Partnership
Devizes Town Council
Kennet Community Safety Partnership
Wiltshire Constabulary

Code of Practice in respect of the Operation of
Devizes Development Partnership CCTV Surveillance System

Code of Practice

Devizes Development Partnership
CCTV Surveillance System

ACKNOWLEDGEMENT

This Code of Practice is based upon the CCTV User Group Model Code of Practice.

The Model Code has been developed with the assistance of CCTV users across the country.

Devizes Development Partnership wishes to acknowledge the help and assistance provided by the CCTV User Group and its members in formulating this Code and allowing it to be used as the basis for this Code.

Details of the formulation, application and liability for the CCTV User Group Model Code of Practice are shown in **Appendix J**.

Section 1 Introduction and Objectives

1.1 Introduction

1.1.1 A Closed Circuit Television (CCTV) system has been introduced in Devizes Town Centre. This system known as the Devizes Development Partnership CCTV Surveillance System (the System), comprises a number of cameras installed at strategic locations. These cameras are fully operational with pan, tilt and zoom facilities. There are recording facilities at the CCTV monitoring room.

1.1.2 Section 163 of the Criminal Justice and Public Order Act 1994 confers the power for local authorities to provide *'apparatus for recording visual images of events occurring on any land in their area'* for the purposes of crime prevention and the promotion of the welfare of victims of crime. In addition there is a duty incumbent on all local authorities *'to do all that it reasonably can to prevent crime and disorder in its area'*, s.17 Crime and Disorder Act 1998.

1.1.3 In furtherance of these objectives Kennet District Council (KDC) has agreed to enter into an Agreement with the D.D.P. (Trading) Limited (DDP) who shall operate the System with the assistance of the Devizes Town Council, Kennet Community Safety Partnership, Devizes Community Area Planning Partnership, Wiltshire Constabulary and retailers and businesses in the town who have all certified their acceptance of this code (the 'Partnership'), whereby DDP will provide the System in accordance with the Agreement and this Code of Practice and Procedural Manual with the assistance of the other members of the Partnership.

1.1.4 For the purposes of this document, the 'owner' of the system is the DDP.

1.1.5 Each of the Partnership members shall be required to give a formal undertaking, by way of the execution of a Code of Practice Compliance Declaration (at Appendix E), that they will comply with this Code of Practice and act in good faith with regard to the principles which it embodies. KDC will retain the original of each of these declarations.

1.1.6 For the purposes of the Data Protection Act 1998 there are 2 'Data Controllers' being KDC and the DDP (the DDP also being the Data Processor of the data captured), both of which have notified the Information Commissioners Office (ICO) of the existence of the System. Note:- The **data controller** is the person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data is to be processed. It must be a legal entity e.g. person, organisation or

corporate body and in the case of partnerships all partners may be considered to bear the responsibility.

1.1.7 The 'System Manager' is the DDP Town Centre Manager.

1.1.8 Details of key personnel, their responsibilities and contact points are shown at **Appendix A** to this Code.

1.2 Partnership statement in respect of the Human Rights Act 1998

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

1.2.2 It is recognised that operation of the System may be considered to infringe on the privacy of individuals. KDC and the Partnership recognises that it is their responsibility to ensure that the scheme should always comply with all relevant legislation, including but not limited to the Human Rights Act 1998 and the Data Protection Act 1998 in order to ensure its existing and continued legality and legitimacy. The scheme will only be used as a proportionate measure to achieve the aims and objectives outlined in this Code of Practice and be used only in so far as it is necessary in a democratic society, to increase public safety, for the economic well being of the area, for the prevention and detection of crime and disorder, for the protection of health and morals and/or for the protection of the rights and freedom of others.

1.2.3 The Codes of Practice and observance of the Operational Procedures hereinafter made reference to shall ensure that evidence is secured, retained and made available in such a way as to ensure there is absolute respect for everyone's rights under the Human Rights Act 1998 including but not limited to the right to respect for one's private life and the right to a fair trial.

1.3 The Procedural Manual

1.3.1 This Code of Practice (hereafter referred to as 'the Code) is supplemented by a separate 'Procedural Manual' which offers instructions on all aspects of the day to day operation of the System. To ensure the purpose and principles (see Section 2) of the System are realised, the Procedural Manual is based and expands upon the contents of this Code of Practice. The Procedural Manual is annexed at Appendix N.

1.4 Objectives of the System

1.4.1 The objectives of the System as determined by KDC and the Partnership are:-

- To help reduce the fear of crime.
- To help deter crime.
- To help detect crime and provide evidential material for court proceedings.
- To assist in the overall management of Devizes Town Centre.
- To enhance community safety, assist in developing the economic well being of the area and encourage greater use of the facilities in the town.
- To assist KDC in its enforcement and regulatory functions within the town.
- To assist in traffic management.
- To assist in supporting civil proceedings which will help detect crime.
- To assist other emergency services.

Section 2 Statement of Purpose and Principles

2.1 Purpose

2.1.1 The purpose of this document is to set out the Partnership's intentions and objectives as regards the System and how these intentions and objectives are to be realised. This document also seeks to outline how the System is to operate within the legal constraints imposed on such a project.

2.1.2 The purpose of the System and the process adopted in determining the reasons for implementing the System are as previously defined in order to achieve the objectives detailed within Section 1.

2.2 General Principles of Operation

2.2.1 The System will be operated in accordance with all the requirements and the principles of the Human Rights Acts 1998 and Data Protection Act 1998 and the terms of this Code of Practice and the Information Commissioner's Office CCTV Code of Practice.

2.2.2 The Partnership recognises the need for formal authorisation for the operation of directed surveillance and intrusive surveillance (as defined by s.26 Regulation of Investigatory Powers Act 2000 (RIPA)), as required by RIPA and the police force policy

Notes

1. The installation of a CCTV camera is considered to **be overt** unless it is installed in a manner whereby its presence is deliberately intended to be concealed from the view of any person likely to be within the field of view of that camera.
2. Cameras which may be placed in domes or covered to reduce the likelihood of assessing their field of view, or to protect them from weather or damage, would not be regarded as covert provided that appropriate signs indicating the use of such cameras are displayed in the vicinity.

2.2.3 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.

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

2.2.5 Any organisation, individual or authority who wishes to be involved in the operation of the System or involved in any way in respect of the System must express their adherence to this Code by means of the entering into of a signed Deed of Adherence, annexed at Appendix L.

2.2.6 Subject to permitted use modifications agreed in accordance with this Code of Practice the use of the System shall be restricted to the following general purposes:-

2.2.6.1 To assist the prevention and detection of crime and offences and to assist the Police with the more efficient deployment of resources for the purpose of deterring crime and apprehending criminals.

2.2.6.2 The provision of evidence for the prosecution of criminals.

2.2.6.3 To assist the tracking and apprehension of persons who are suspected of having committed a criminal offence.

2.2.6.4 To assist the prevention and detection of anti-social behaviour which is or is likely to prevent law-abiding members of the community from freely expressing their right to make use of the areas of CCTV coverage without fear or hindrance.

2.2.6.5 To assist in the general planning and management of the areas of CCTV coverage for the purpose of enhancing their use and enjoyment by the public.

2.2.6.6 To assist the identification and compilation of information which can be used to ensure the safety of the public.

2.2.6.7 To assist the fire, ambulance and civil emergency service with the efficient deployment of their resources to deal with emergencies.

2.2.6.8 To assist the management and efficiency of public services in the area of CCTV coverage.

2.2.6.9 To identify bylaw contraventions.

2.3 Copyright

2.3.1 Copyright and ownership of all material recorded by virtue of the System will remain in the joint legal ownership of the Data Controllers.

2.4 Cameras and Area Coverage

2.4.1 The areas covered by the System to which this Code of Practice refers are the public areas within the responsibility of the Partnership members and cover Devizes Town Centre.

2.4.2 From time to time transportable or mobile cameras may be temporarily sited within the Town Centre of Devizes. The use of such cameras, and the data produced by virtue of their use, will always accord with the objectives of the System and be governed by this Code and all associated procedures, including but not limited to the Procedural Manual.

2.4.3 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.

2.4.4 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 KDC and the Partnership acknowledge that the presence of all cameras must and will be identified by appropriate signs.

2.5 Monitoring and Recording Facilities

2.5.1 A volunteer staffed monitoring room is located at The Crown Centre, 39 St John's Street. The CCTV equipment has the capability of recording all cameras simultaneously throughout every 24 hour period.

2.5.2 Secondary monitoring equipment may be located in police premises. No equipment, other than that housed within the main CCTV control room shall be capable of recording images from any of the cameras.

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

2.6 Human Resources

2.6.1 Unauthorised persons will not have access without an authorised member of staff being present.

2.6.2 The monitoring room shall be staffed by specially selected and trained volunteer operators in accordance with the strategy contained within the procedural manual.

2.6.3 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 associated procedures. Further training will be provided as necessary.

2.7 Processing and Handling of Recorded Material

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

2.8 Operators Instructions

2.8.1 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 Procedural Manual

2.9.1 Any major changes to either the Code of Practice of the Procedural Manual will be effected only after consultation with and the written agreement of KDC and all Partnership members.

2.9.1.1 Major changes to this Code and/or the Procedural Manual can be defined as changes which affect its fundamental principles and objectives and shall be deemed to include such things as:-

- Matters which have data protection and privacy implications
- Additions to the permitted uses criteria
- Changes in the right of access to recorded material

2.9.2 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 Owner of the System after consultation with KDC and the Partnership members the Owner and the System Manager being required to have due regard to the responses of the same.

2.9.2.1 Minor changes to this Code and/or Procedural Manual can be defined as changes of an operational and procedural nature and which do not affect the fundamental principles of objectives underpinning the System and shall be deemed to include such things as:-

- Additions and omissions of cameras to the System.
- Additional clarification and explanations and corrections to the existing Code.
- Additions to the Code in order to conform to the requirements of any statutory Acts and changes in criminal legislation.

Section 3 Privacy and Data Protection

3.1 Public Concern

3.1.1 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.

Note: 'Processing means **obtaining, recording** or **holding** the information or data or **carrying out any operation** or **set of operations** on the information or data, including:-

i) organisation, adaptation or alteration of the information or data;
ii) retrieval, consultation or use of the information or data;
iii) disclosure of the information or data by transmission, dissemination or otherwise making available, or
iv) alignment, combination, blocking, erasure or destruction of the information or data.

3.1.2 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 there will be total respect for everyone's right to respect for his or her private and family life and their home.

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

3.1.4 Each Partnership member, organisation and person with access to any data captured and/or stored shall sign a formal confidentiality declaration (annexed at Appendix E) that they will treat any viewed and/or written material as being strictly confidential and that they undertake not to divulge it to any other person

3.2 Data Protection Legislation

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

i) All personal data will be obtained and processed fairly and lawfully.
ii) Personal data will be held only for purposes specified.
iii) Personal data will be used only for the purposes, and disclosed only to the people shown within these codes of practice.
iv) Only personal data will be held which are adequate, relevant and not excessive in relation to the purpose for which the data are held.

v) Steps will be taken to ensure that personal data are accurate and where necessary kept up to date.
vi) Personal data will be held no longer than is necessary.
vii) Individuals will be allowed access to information held about them and, where appropriate, permitted to correct or erase it.

Procedures will be implemented to put in place security measures to prevent unauthorised or accidental access to, alteration, disclosure, or loss and destruction of, information.

3.2.2 The 'data controllers' of the System are KDC and Devizes Development Partnership whilst day to day responsibility for the control and processing of the data will be devolved to the CCTV Manager. The ICO has been notified in accordance with current data protection legislation.

3.3 Freedom of Information

3.3.1 The DDP acknowledges that KDC is subject to the Freedom of Information Act 2000 and shall do all it can in order to help and assist KDC in complying with this legislation including but not limited to ensuring that any information request received by the DDP is passed to KDC promptly and the provision of any information requested and required to be disclosed by KDC is made available promptly

3.4 Recorded Material

3.4.1 For the purposes of this Code 'Recorded Material' means any material recorded by technical equipment which forms part of the System, and specifically includes images recorded digitally, or on videotape or by way of video or DVD copying, including image prints.

3.4.2 Every video or digital recording obtained by using the System has the potential of containing material that may be admitted in evidence.

3.4.3 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.

3.4.4 It is therefore of the utmost importance that irrespective of the means or format (e.g. paper, copy, video tape, DVD, CD or any form or electronic processing and storage) of the images obtained from the System, they are treated strictly in accordance with this Code of Practice and the Procedural Manual from the moment they

are received by the monitoring room until final destruction. Every movement and usage will be meticulously recorded.

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

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

3.5 Request for Information (Subject Access)

3.5.1 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.

3.5.2 The principles of Sections 7 and 8, 10 and 12 of the Data Protection Act 1998 (Rights of Data Subjects and Others) shall be followed in respect of every request. These Sections are reproduced as Appendix B to this code.

3.5.3 If the request cannot be complied with without identifying another individual, permission from all parties must be considered (in the context of the degree of privacy they could reasonably anticipate from being in that location at that time) in accordance with the requirements of the legislation. If permission is not obtained the data shall not be released without adequate and sufficient steps being taken to prevent the release of personal data and if the steps taken are not sufficient to protect this data, the data shall not be released.

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

3.6 Exemptions to the Provision of Information

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

"Personal data processed for any of the following purposes -

i) the prevention or detection of crime

ii) the apprehension or prosecution of offenders

are exempt from the subject access provisions in any case ' to the extent to which the application of those

provisions to the data would be likely to prejudice any of the matters mentioned in this subsection'.

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

3.7 Criminal Procedures and Investigations Act 1996

3.7.1 The Criminal Procedures and Investigations Act 1996 came into effect in April 1997 and introduced a statutory framework for the disclosure to defendants of material which the prosecution would not intend to use in the presentation of its own case, (known as unused material). Disclosure of unused material under the provisions of this Act should not be confused with the obligations placed on the data controller by Section 7 of the Data Protection Act 1998, (known as subject access).

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

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

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

- Recorded material shall be processed lawfully and fairly, and used only for the purposes defined in this Code of Practice;
- Access to recorded material will only take place in accordance with the standards outlined in Appendix C and this Code of Practice:
- The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

3.8.3 Members of the police service or other agency having a statutory authority to investigate and / or prosecute offences may, subject to compliance with Appendix C, release details of recorded information to the media only in an effort to identify alleged offenders or potential witnesses. Under such circumstances, full details will be recorded in accordance with the Procedural Manual.

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

3.8.4 If material is to be shown to witnesses, including police officers, for the purpose of obtaining identification evidence, it must be in accordance with Appendix C and the Procedural Manual.

3.8.5 It may be beneficial to make use of 'real' digital 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 bona fide training and education purposes. Recorded material will not be released for commercial or entertainment purposes.

3.9 Recording Policy

3.9.1 Subject to the equipment functioning correctly, images from every camera will be recorded throughout every 24 hour period through digital multiplexers directly onto the DVD hard drive.

3.9.2 Images from selected cameras will be recorded in real time at the discretion of the CCTV operators or as directed by the CCTV Manager.

3.9.3 Recordings on the DVD hard drive will be stored for a minimum of 14 days.

3.9.4 Copies of recordings either on DVDs or videos will be used, stored or destructed strictly in accordance with the procedures outlined in the Procedural Manual.

3.10 Evidential Purposes

3.10.1 In the event of a recording being required for evidential purposes the procedures outlined in the Procedural manual will be strictly complied with.

3.11 Video Prints

3.11.1 A video print is a copy of an image or images which already exists on computer hard drive, DVDs or videos tapes. Such prints are equally within the definitions of ‘data’ and recorded material.

3.11.2 Video prints will not be taken as a matter of routine. Each time a print is made it must be capable of justification by the originator who will be responsible for recording and the full circumstances under which the print is taken in accordance with the Procedural Manual.

3.11.3 Video prints contain data and will therefore only be released under the terms of Appendix C to the Code of Practice, ‘Release of Data to Third parties’. If prints are released to the media, (in compliance with Appendix C), in an effort to identify alleged offenders or potential witnesses, full details will be recorded in accordance with the Procedural Manual.

3.11.4 A record will be maintained of all video print productions in accordance with the Procedural Manual. The recorded details will include: a sequential number, the date, time and location of the incident, date and time of the production of the print and the identity

of the person requesting the print, (if relevant) and the purpose for which the print was taken.
The records of the video prints taken will be subject to audit in common with all other records in the system.

Section 4 Accountability and Public Information

4.1 The Public

4.1.1 For reasons of security and confidentiality, access to the CCTV monitoring room is restricted in accordance with this Code of Practice. However, in the interest of openness and accountability anyone wishing to visit the room may be permitted to do so, subject to the approval of, and after making prior arrangements with the System Manager.

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

4.1.3 A member of the public wishing to register a complaint with regard to any aspect of the System may do so by contacting the CCTV Manager's office. All complaints shall be dealt with in accordance with the DDP's complaints procedure, a copy of which may be obtained from the CCTV Manager.

4.1.4 All CCTV voluntary staff are subject to regulations governing confidentiality and discipline.

4.2 System Owner

4.2.1 The DDP Chairman named at Appendix A, being the nominated representative of the Owners of the System, will have unrestricted access to the CCTV monitoring room and will be responsible for receiving regular and frequent reports from the System Manager.

4.2.2 The DDP Executive will nominate a CCTV Forum committee with representatives from the partnership organisations with the specific responsibility for receiving and considering those reports.

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

4.3 System Manager

4.3.1 The DDP Chairman and the CCTV Manager, named at Appendix A will have day to day responsibility for the system as a whole.

4.3.2 The System will be subject to annual audit, by the CCTV User Group under its Accreditation by Assessment Scheme.

4.3.3 The CCTV Manager will ensure that every complaint is acknowledged in writing within five working days which will include advice to the complainant of the enquiry procedure to be taken. A formal report will be forwarded to the nominee of the system owner named at Appendix A, giving details of all complaints and the outcome of relevant enquiries.

Note:
An informal foreshortened process whereby the System Manager informs the system owners of any complaint within 7 working days would be considered Best Practice.

4.3.4 Statistical and other relevant information, including any complaints made, will be included in the DDP CCTV Annual Report, and are publicly available.

4.4 Public Information

4.4.1 A copy of this Code of Practice will be published on DDP's and KDC's website and a copy will be made available to anyone on request. Additional copies will be lodged at Devizes Library, Devizes Police Station and Council reception offices.

4.4.2 Annual Report

The DDP CCTV Annual Report and that for subsequent years shall be published by the end of June in the year following the reporting year. A copy of the annual report will also be made available to anyone requesting it. Additional copies will be lodged at Devizes Library, Devizes Police Station and council reception offices.

4.4.3 Signs

Signs will be placed in the locality of the cameras and at the main entrance points to the relevant areas and shall be in the form of the nationally recognised sign developed by the CCTV User Group. The signs will indicate:-

i) The presence of CCTV monitoring;
ii) The 'ownership' of the system;
iii) Contact telephone number of the 'data controller' of the system.

Note: The nationally recognised sign developed by The CCTV User Group is in use by organisations throughout the UK. The design and wording has been approved by the Standards Committee of The CCTV User Group and been accepted by the Department of Transport (Advertising Section). The sign has also been assessed by the Office of the Information Commissioner and the Police Scientific Development Branch of the Home Office.

Section 5 Assessment of the System and Code of Practice

5.1 Evaluation

5.1.1 The System will periodically be independently evaluated to establish whether the purposes of the System are being complied with and whether objectives are being achieved. The format of the evaluation shall comply with that laid down by the Home Office statistics and Research Directorate in the Home Office Bidding Guidelines and be based on assessment of the Inputs, the Outputs, The Process and the Impact of the Scheme.

i) An assessment of the impact upon crime: This assessment shall include not only the immediate area covered by the cameras but the wider town area, the Police Divisional and regional areas and national trends.
ii) An assessment of the incidents monitored by the system.
iii) An assessment of the impact on town centre businesses.
iv) An assessment of neighbouring areas without CCTV.
v) The views and opinions of the public.
vi) The operation of the Code of Practice.
vii) Whether the purposes for which the system was established are still relevant.
viii) Cost effectiveness.

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

5.1.3 It is intended that evaluations should take place every two years.

5.2 Monitoring

5.2.1 The CCTV Manager will accept day to day responsibility for the monitoring, operation and evaluation of the system and the implementation of the Code.

5.2.2 The CCTV 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

5.3.1 The DDP Executive Committee will be responsible for regularly auditing the operation of the system and the compliance with this Code of Practice. Audits, which may be in the form of irregular spot checks, will include examination of the monitoring room records, video tape and DVD histories and the content of recorded material. The Audit report will be made available on request.

5.4 Inspection

5.4.1 A body of individuals who have no direct contact or relationship with the operation of the system have been appointed to be responsible for inspecting the operation of the system. Inspections will take place at least six times per calendar year by no more than two people at any one time. The inspectors will be permitted access to the CCTV monitoring room, without prior notice and to the records held therein at any time, provided their presence does not disrupt the operational functioning of the room. Their findings will be reported to the Auditor and their visit recorded in the CCTV monitoring room. Reports will be drafted and made available to the public.

5.4.2 Inspectors will be required to sign a declaration of confidentiality. (See Appendix F).

5.5 Complaints Procedure

5.5.1 A complaints procedure will be established to allow the public and anyone affected by the operation of the System to formally raise any issue which is causing concern.

5.5.2 Complaints should initially be made to the CCTV Manager at the address listed in Appendix A. All complaints will be acknowledged in writing within 3 working days and will receive a detailed response within 20 working days.

5.5.3 All complaints will be reported to Kennet District Council.

5.5.4 The Complaints Procedure is annexed at Appendix K.

Section 6 Control and Operation of Cameras

6.1 Guiding principles

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

6.1.2 The System shall only be used for the purposes outlined in this Code.

6.1.3 Cameras will not be used to look into private residential property. 'Privacy Zones' shall be programmed into the system (whenever practically possible) in order to ensure that the interior of any private residential property within range of the system is not surveyed by the cameras.

6.2 Staffing of the Monitoring Room and those responsible for the operation of the System

6.2.1 The CCTV Monitoring Room will be staffed in accordance with the **Procedural Manual.** Equipment associated with the System will only be operated by authorised personnel who have been properly trained in its use and monitoring room procedures and shall only be used for the purposes outlined in this Code of Practice.

6.2.2 Every person involved in the management and operation of the System will be personally issued with a copy of both the Code of Practice and the Procedural Manual, will be required to sign a confirmation that they fully understand the obligations placed on them and certify that they adhere to these documents and that any breach will be considered a disciplinary offence. They will be fully conversant with the contents of both documents, which may be updated from time to time, and which he / she will be expected to comply with at all times.

6.2.3 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 with this Code of Practice and associated Procedural Manual.

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

6.3 Discipline

6.3.1 Every individual with any responsibility under the terms of this Code of Practice and who has any involvement with the System, will be

subject to the DDP's discipline code (the Discipline Code) annexed at Appendix M. Any breach of this Code of Practice or of any aspect of confidentiality will be dealt with in accordance with those discipline rules.

6.3.2 The CCTV Manager will accept primary responsibility for ensuring there is no breach of security and that the Code of Practice is complied with. He / she has day to day responsibility for the management of the room and for enforcing compliance with the Discipline Code. Non-compliance with this Code of Practice by any person will be considered a severe breach of discipline and dealt with according to the Discipline Code.

6.4 Declaration of Confidentiality

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

6.5 Operational Command of the System by the Police

6.5.1 Under rare and extreme operational circumstances the Police may make a request to command the use of the System to which this Code of Practice applies. These circumstances may be a major incident or event that has a significant impact on the prevention and detection of crime of public safety.

6.5.2 Such requests will be viewed separately to the use of the systems' cameras with regard to the requirement for an authority for specific types of surveillance under the Regulation of Investigatory Powers Act 2000. (See Appendix I).

6.5.3 Request made as at 6.5.1 will be considered on the written authority of a police officer not below the rank of Superintendent. Any such request will only be accommodated on the personal written authority of the most senior representative of the System owners, or designated deputy of equal standing. In the event or urgent need the verbal authority of the senior officer in charge, and in any event, an officer not below the rank of an Inspector will be necessary. This should be followed as soon as practicable by a Superintendents authority in any event within 72 hours.

6.5.4 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 trained and authorised to do so, and who fall within the terms of Sections 6 and 7 of this Code. They will then operate under the command of the police officer designated in the

verbal / written authority, taking into account their responsibilities under this code.

6.5.5 In very extreme circumstances a request may be made for the Police to take total control of the System in its entirety, including the staffing of the monitoring room and personal control of all associated equipment, to the exclusion of all representatives of the System owners. Any such request should be made to the CCTV Manager in the first instance, who will consult personally with the most senior officer of the System owners (or designated deputy of equal standing). A request for total exclusive control must be made in writing by a police officer not below the rank of Assistant Chief Constable or person of equal standing.

Section 7 Maintenance of the System

7.1 To ensure compliance with the Information Commissioners Code of Practice and that images recorded continue to be of appropriate evidential quality the System shall be maintained in accordance with the requirements of the Procedural Manual.

7.2 The maintenance agreement will make provision for regular / periodic service checks on the equipment which will include cleaning of any all weather domes or housings, checks on the functioning of the equipment, and any minor adjustments that need to be made to the equipment settings to maintain picture quality.

7.3 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.

7.4 The maintenance agreement will also provide for 'emergency' attendance by a specialist CCTV engineer on site to rectify any loss or severe degradation of image or camera control.

7.5 The maintenance agreement will define the maximum periods of time permitted for attendance by the engineer and for rectification of the problem depending upon the severity of the event and the operational requirements of that element of the system.

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

Section 8 Access to and Security of, Monitoring Room and Associated Equipment

8.1 Authorised Access

8.1.1 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

8.2.1 Public access to the monitoring and recording facility will be prohibited except for lawful, proper and sufficient reasons and only then with the personal authority of the System Manager. Any such visits will be conducted and recorded in accordance with the Procedural Manual.

8.3 Authorised Visits

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

8.4 Declaration of Confidentiality

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

"In signing this visitors book all visitors to this CCTV monitoring room acknowledge all information should remain confidential. They further agree not to divulge any information obtained, overheard or overseen during their visit".

A notice is displayed at the entrance to the room that they are entering a restricted area, and entry is dependent upon acceptance of the need for confidentiality. A copy notice is included in Appendix D.

8.5 Security

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

8.5.2 The monitoring room will at all times be secured.

APPENDIX A KEY PERSONNEL AND RESPONSIBILITIES

1. System Owners

Chairman
Devizes Development Partnership
C/o J S Weeks & Co
41 St John's Street
Devizes, SN10 1BL

Responsibilities:-

Devizes Development Partnership, acting through its Chairman, is the 'Owner' of the System. The Chairman's role will include a responsibility to:-

i) Ensure the provision and maintenance of all equipment forming part of the System in accordance with contractual arrangements which the Owners may from time to time enter into with the agreement of KDC and the Partnership.
ii) Maintain close liaison with the System Manager.
iii) Ensure the System is operated in accordance with the terms of this Code of Practice.
iv) Consult with, where necessary, KDC and the Partnership in relation to any proposed alterations and additions to the System, this Code of Practice and / or the Procedural Manual and where the Code of Practice allows make decisions on behalf of the Partnership.

2. System Management

The CCTV Control
The Crown Centre
St John's Street
Devizes

Responsibilities:-

The CCTV Manager is the 'System Manager' of the CCTV System.
The 'System Manager' has delegated authority for data control on behalf of the 'data controllers'. The role includes responsibility to:-

i) Maintain day to day management of the System and volunteers.
ii) Accept day to day responsibility for the System and for ensuring that this Code of Practice is complied with.
iii) Maintain direct liaison with the owners of the System.
iv) Maintain direct liaison with operating partners.

APPENDIX B EXTRACTS FROM DATA PROTECTION ACT 1998

Section 7

(1) Subject to the following provisions of this section and to Sections 8 and 9, an individual is entitled to:

a) To be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller.

b) If that is the case, to be given by the data controller a description of:-

i) The personal data of which that individual is the data subject;

ii) The purpose for which they are being or are to be processed;

iii) The recipients or classes of recipients to whom they are or may be disclosed.

c) To have communicated to him / her in an intelligible form:

i) The information constituting any personal data of which that individual is the subject data;

ii) Any information available to the data controller as the source of those data.

d) Where the processing by automatic means of personal data of which that individual is the data subject for the purposes of evaluating matters relating to him / her such as, for example, his / her performance at work, his / her creditworthiness, his / her reliability or his / her conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him / her, to be informed by the data controller of the logic involved in that decision making.

(2) A data controller is not obliged to supply any information under subsection (1) unless he / she has received:-

a) A request in writing, and

b) Except in prescribed cases, such fee (not exceeding the prescribed maximum) as he / she may require.

(3) A data controller is not obliged to comply with the request under this section unless he / she is supplied with such information as he / she may reasonably require in order to satisfy hi / herself as to the identity of the person making the request and to locate the information which that person seeks.

(4) Where a data controller cannot comply with the request without disclosing information relating to another individual who can be identified from that information, he / she is not obliged to comply with the request unless:-

a) The other individual has consented to the disclosure of the information to the person making the request, or

b) It is reasonable in all circumstances to comply with the request without the consent of the other individual.

(5) In subsection (4) the reference to information relating to another individual includes a reference to information identifying that individual as the source of information sought by the request; and that subsection is not to be construed as excusing the data controller from communicating so much of the information sought by the request as can be communicated without disclosing the identity of the other individual concerned, whether by omission of names or other identifying particulars or otherwise.

(6) In determining for purposes of subsection (4)(b) whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned, regard shall be had, in particular to:-

a) Any duty of confidentiality owed to the other individual;
b) Any steps taken by the data controller with a view to seeking the consent of the other individual;
c) Whether the other individual is capable of giving consent;
d) Any express refusal of consent by the other individual.

Note: *In considering such instances the data controller must effectively also consider the degree of privacy that the third parties might or might not reasonably expect in being at that location at that time.*

(7) An individual making a request under this section may, in such cases as may be prescribed, specify that his / her request is limited to personal data of any prescribed description.

(8) Subject to subsection (4), a data controller shall comply with a request under this section promptly and in any event before the end of the prescribed period beginning with the relevant day.

(9) If a court is satisfied on the application of any person who has made a request under the forgoing provisions of this section that the data controller in question has failed to comply with the request in contravention of those provisions, the court may order him / her to comply with the request.

In this section:-

'prescribed' means prescribed by the Secretary of State by regulations;
'the prescribed maximum' means such amount as may be prescribed;
'the prescribed period' means forty days or such other period as my be prescribed;
'the relevant day', in relation to a request under this section, means the day on which the data controller receives the request or, if later, the first day on which the data controller has both the required fee and the information referred to in subsection (3).

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

Section 8

(1) The Secretary of State may by regulations provide that, in such cases as may be prescribed, a request for information under any provision of subsection 910 of section 7 is to be treated as extending also to information under other provisions of that subsection.

(2) The obligation imposed by section 7 (1)(c)(i) must be complied with by supplying the data subject with a copy of the information in a permanent form unless:-

a) The supply of such a copy is not possible or would involve disproportionate effort, or;
b) The data subject agrees otherwise;
c) And where any of the information referred to section (7)(c)(i) is expressed in terms which are not intelligible without explanation the copy must be accompanied by an explanation of those terms.

(3) Where a data controller has previously complied with a request made under section 7 by an individual, the data controller is not obliged to comply with a subsequent identical or similar request under that section by that individual unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request.

(4) In determining the purposes of subsection (3) whether request under section 7 are made at reasonable intervals, regard shall be had to the nature of the data, the purpose for which the data are processed and the frequency with which the data are altered.

(5) Section 7(1)(d) is not to be regarded as requiring the provision of information as to the logic involved in decision-taking if, and to the extent that, the information constitutes a trade secret.

(6) The information to be supplied pursuant to request under section 7 must be supplied by reference to the data in question at the time when the request is received, except that it may take account of any amendment or deletion made between that time and the time when the information is supplied, being an amendment or deletion that would have been made regardless of the receipt of the request.

(7) For the purposes of section 7 (4) and (5) another individual can be identified from the information being disclosed if he / she can be identified from that information, or from that and any other information which, in the reasonable belief of the data controller, is likely to be in, or to come into, the possession of the data subject making the request.

Note: *These extracts are for initial direction and guidance only. To ensure compliance with the legislation the relevant Data Protection legislation should be referred to in its entirety. Copies of the act and the Information Commissioners Code of Practice can be downloaded from their website.*

www.ico.gov.uk

APPENDIX C NATIONAL STANDARD FOR THE RELEASE OF DATA TO THIRD PARTIES

(1) Introduction

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

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

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

(2) General Policy

All requests for the release of data shall be processed in accordance with the Procedural Manual. All such requests shall be channelled through the data controller.

Note: *The data controller is the person who (either alone or jointly with others) determines the purpose for which and the manner in which any personal data are, or are to be processed. (In most cases the data controller is likely to be the scheme owners or for a 'partnership' the partners share responsibility). Day to day responsibility may be devolved, usually to the scheme manager.*

(3) Primary Request to View Data

a) Primary request to view data generated by a CCTV System are likely to be made by third parties for any one or more of the following purposes:-

- i) Providing evidence in criminal proceedings (e.g. Police and Criminal Evidence Act 1984, Criminal Procedures 7 Investigations Act 1996, etc.);
- ii) Providing evidence in civil proceedings or tribunals;
- iii) The prevention of crime;
- iv) The investigation and detection of crime (may include identification of offenders);
- v) Identification of witnesses.

b) Third parties, which are required to show adequate grounds for disclosure of data within the above criteria, may include, but are not limited to:-

i) Police (1)
ii) Statutory authorities with powers to prosecute, (e.g. customs and Excise; trading standards, etc.)
iii) Solicitors (2)
iv) Plaintiffs in civil proceedings (3)
v) Accused persons or defendants in criminal proceedings (3)
vi) Other agencies, according to purpose and legal status (4)

c) Upon receipt from a third party of a bona fide request for the release of data, the 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) In circumstances outlined at note (3) below, (requests by plaintiffs, accused persons or defendants) the data controller, or nominated representative, shall:-
   i) Be satisfied that there is no connection with any existing data held by the police in connection with the same investigation.
   ii) Treat all such enquiries with strict confidentiality.

Notes

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

(2) Aside from criminal investigations, data may be of evidential value in respect of civil proceedings or tribunals. In such cases a solicitor, or authorised representative of the tribunal, is required to give relevant information in writing prior to a search being granted. In the event of a search resulting in a requirement being made for the release of data, such release will only be facilitated on the instructions of a court order or subpoena. A charge may be made for this service to cover costs incurred. In all circumstances data will only be released for lawful and proper purposes.

(3) There may be occasions when an enquiry by a plaintiff, an accused person, a defendant or a defence solicitor falls outside the terms of disclosure or subject access legislation. An example could be the investigation of an alibi. Such an enquiry may not form part of a prosecution. Defence enquiries could also arise in a case where there appeared to be no recorded evidence in a prosecution investigation.

(4) The data controller shall decide which (if any) 'other agencies' might be permitted access to data. Having identified those 'other agencies', such access to data will only be permitted in compliance with this standard.

(5) The data controller can refuse an individual request to view if insufficient or inaccurate information is provided. A search request should specify reasonable accuracy (could be specified to the nearest ½ hour).

(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 & 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 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 into 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.

ii) If the material is to be released under the auspices of 'public well being, health or safety, written agreements to the release of material should be obtained from the DDP Chairman.

c) Recorded material may be used for bona fide training purposes such as police or volunteer training. Under no circumstances will recorded material be released for commercial sale of material for training or entertainment purposes.

Note:-

(1) 'Disclosure in the public interest could include the disclosure of personal data that:-

i) Provides specific information which would be of value or of interest to the police well being;

ii) Identifies a public health or safety issue;

iii) Leads to the prevention of crime;

iv) The disclosure of personal data which is the subject of a 'live' criminal investigation would always come under the terms of a primary request.

5 Individual Subject Access under Data Protection Legislation

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

i) The request is made in writing;

ii) A specified fee is paid for each search;

iii) The data controller is supplied with sufficient information to satisfy him or herself 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 him or herself 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 controlled 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 that the audit trail has been maintained;

v) Not removed or copied without proper authority;

vi) For individual disclosure only (i.e. to be disclosed to a named subject).

6. Process of Disclosure

a) Verify the accuracy of the request.

b) Replay the data to the person making the request 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).

e) If a copy of the material is requested and there is no on-site means of editing out the other personal data, then the material shall be sent to an editing house for processing prior to being sent to the person making the request.

Note:- *The Information Commissioners Code of Practice makes specific requirements for the precautions to be taken when images are sent to an editing house for processing.*

7 Media Disclosure

In the event of a request from the media for access to recorded material, the procedures outlined under 'secondary request to view data' shall be followed. If material is to be released the following procedures shall be adopted:-

i) The release of the material must be accompanied by a signed release document that clearly states what the data will be used for and sets out the limits on its use.

ii) The release form shall state that the receiver must process the data in a prescribed manner 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 signed by both parties. (1)

Notes:-

(1) In the well publicised case of R v Brentwood Borough Council, ex parte Geoffrey Dennis Peck, (QBD November 1997), the judge concluded that by releasing the video footage, the Council had not acted lawfully. 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.

Attentions is drawn to the requirements of the Information Commissioners in this respect – detailed in the Code of practice summarised above.

8. Principles

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

a) Recorded material shall be processed lawfully and fairly and used only for the purposes defined in the Code of Practice for the CCTV Scheme;

b) Access to recorded material shall only take place in accordance with this Standard and the Code of Practice;

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

APPENDIX D 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 being permitted entry to this area you acknowledge all information should remain confidential. You agree not to divulge any information obtained, overheard or overseen during your visit. An entry accompanied by your signature in the Visitors book is your acceptance of these terms'.

APPENDIX E DECLARATION OF CONFIDENTIALITY

Devizes Development Partnership CCTV System

1, …… have volunteered to perform the duties of a CCTV Operator for the Devizes Development Partnership CCTV System. I have received a copy of the Code of Practice in respect of the operation and management of the 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 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 the same.

I understand that it is a condition of voluntary participation that I do not disclose or divulge to any individual, firm, company, authority, agency or other organisation, any information which I may have acquired in the course of, or for the purposes of, my position in connection with the CCTV System, verbally, in writing or by any other media, now or in the future, (including such time as I may 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 and Procedural Manual 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 ……

Date ……

APPENDIX F INSPECTORS DECLARATION OF CONFIDENTIALITY

In respect of the Devizes Development Partnership CCTV System

I, …….. am a voluntary inspector of the System with a responsibility to monitor the operation of the System and adherence to the Code of Practice. I have received a copy of the Code of Practice in respect of the operation and management of that CCTV System.

I hereby declare that:-

I am fully conversant with my voluntary duties and the content of that Code of Practice. I undertake to inform the System Manager of any apparent contravention of the Code of Practice that I may note during the course of my visits to the monitoring facility.

If now, or in the future I am, or 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 the same.

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

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

Signed ……. Print

Name ……

Witness …….

Position ……

Date ……

APPENDIX G SUBJECT ACCESS REQUEST FORM

DEVIZES DEVELOPMENT PARTNERSHIP
CCTV SURVEILLANCE SYSTEM
Data Protection Act 1998

HOW TO APPLY FOR ACCESS TO INFORMATION
HELD ON THE CCTV SYSTEM

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

Your Rights

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

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

Devizes Development Partnership's Rights

Devizes Development Partnership may deny access to information where the Act allows. The main exemptions in relation to information held on the CCTV System are where the information may be held for:-

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

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

Fee

A fee of £10 is payable for each access request, which must be in pounds sterling. Cheques, postal orders etc should be made payable to:-

Devizes Development Partnership

APPLICATION FORM

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

NOTES

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

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

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

Section 4 **You must sign the declaration.**

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

The CCTV Manager
Crown Centre
St John's St.
Devizes

If you have any queries regarding the form, or your application, please ring the CCTV Manager on 01380 738750.

DEVIZES DEVELOPMENT PARTNERSHIP
CCTV SURVEILLANCE SYSTEM

Data Protection Act 1998

Section 1 About Yourself

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

Title	Mr	Mrs	Miss	Miss
Other Title (Dr, Rev, etc)				
Surname				
First Names				
Maiden name / Previous name(s)				
Sex	Male		Female	
Height				
Date of Birth				
Place of Birth	Town			
	Country			

Current Home Address	
	Post Code
	Tel. No.

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

Previous Address(es)		
Date of Occupancy	From	To
Date of Occupancy	From	To

DEVIZES DEVELOPMENT PARTNERSHIP
CCTV SURVEILLANCE SYSTEM
Data Protection Act 1998

Section 2 Proof of Identity

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

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

Also a recent full face photograph of yourself.

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

Section 3 Supply of Information

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

(a) View the information and receive a permanent copy Yes / No

(b) Only view the information Yes / No

Section 4 Declaration

DECLARATION (to be signed by the applicant)

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

Signed Date

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

Please complete Section 5 overleaf before returning the form

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

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

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

If the information you require relates to a vehicle, property, or other type of information, please complete on a separate sheet.

Were you	(Please tick below)
A person reporting an offence or incident	
A witness to an offence or incident	
A victim of an offence	
A person accused or convicted of an offence	
Other please explain	

Dates(s) and time(s) of incident
Place incident happened
Brief details of incident

DEVIZES DEVELOPMENT PARTNERSHIP
CCTV SURVEILLANCE SYSTEM
Data Protection Act 1998

Before returning this form

- Have you completed ALL sections in this form?

Please check

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

Further information:-

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

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF Tel: 01625 545745

Please note that this application for access to information must be made direct to Devizes Development Partnership and **NOT** to the Data Protection Commissioner.

OFFICIAL USE ONLY	
Date application received	
Fee paid	
Method of payment	
Receipt No.	
Application checked and legible	
Identification documents checked	
Details of 2 documents	
Date documents returned	
Staff signature	
Date	

APPENDIX H AREAS COVERED BY CCTV

The following areas are currently covered by the Devizes Development Partnership CCTV Surveillance System:-

Devizes Town Centre:-

- Market Place
- St Johns Street
- Wine Street
- Little Brittox
- High Street
- The Brittox
- Maryport Street
- Sidmouth Street
- Monday Market Street
- Brewery Corner
- New Park Street

It is the policy of Devizes Development Partnership that CCTV will be introduced throughout the town centre wherever it can be justified.

APPENDIX I REGULATION OF INVESTIGATORY POWERS ACT GUIDING PRINCIPLES

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 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 the part to be sought for the carrying out of the surveillance.

CCTV being used intrusively will be authorised other than by this section of the RIP Act. Appropriate guidelines already exist for intrusive 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 subsection © 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. The code says some hours rather than minutes.

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

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 purposes of preventing or detecting crime or 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 purposes of protecting public health;

f) For the purposes of assessing or collecting any tax, duty, levy or other inspection, 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 forms. Any authority given should be recorded appropriately. This should include the name of the officer authorising.

Forms should be available at the CCTV monitoring centre and are included in the Procedural Manual and available from the CCTV User Group website.

Examples:-

Inspector Authorisation
An example of a request requiring Inspector authorisation might be where a car is found in a car park late at night and known to belong to drug dealers. The officers might task CCTV to watch the vehicle over a period of time to note who goes to and from the vehicle.

Superintendent Authorisation
Where crime squad officers wish to have a shop premises monitored from the outside, which is suspected of dealing in stolen goods, over a period of days.

No Authorisation
Where officers come across a local drug dealer sitting in the town centre / street and wish to have the cameras monitor them, so as not to divulge the observation taking place.

APPENDIX J	FORMULATION, APPLICATION AND LIABILITY FOR THE CCTV USER GROUP MODEL CODE OF PRACTICE AND PROCEDURAL MANUAL

Intention and Formulation of the Model Code of Practice

This Model CCTV Code of Practice intends as far as reasonably practicable, to encourage all 'public area' CCTV systems are operating within the United Kingdom to be compliant with the law and safeguard the integrity of any CCTV System whilst ensuring the right to privacy is not breached.

These codes are complied from CCTV 'best practice' and take account of all legislative changes that effect CCTV. In themselves they are not legally enforceable. They should be used in addition to the Data Protection Act 1998 – Code of Practice issued under The Criminal Procedures & Investigations Act 1996; Codes – Police & Criminal Evidence Act 1994 and draft codes under Regulation of Investigatory Powers Act 2000. Any court or tribunal will only recognise Codes of practice under specific legislation.

Application of the Model Code of Practice

The content of the Model Code of Practice is slanted towards the ownership and management of a 'public area CCTV system'. However, we believe it is equally appropriate to any organisation operating a CCTV system and recommend that all systems, regardless of their complexity, should be compliant with current legislation and regulated by an appropriate Code of Practice. This model is therefore designed to be easily adapted to suit most operational needs.

The model is freely available to all Members of the CCTV User Group and for a nominal charge to non-members on application to the offices of the CCTV User Group.

In any event of any part of the document being deemed inapplicable, it's exclusion should be carefully considered, taking into account the need to safeguard the integrity and credibility of the system and the overriding need to safeguard personal privacy.

CCTV system owners are encouraged to adopt these policy principles and Codes of practice. Owners and managers are invited to reproduce these codes of Practice in whatever format suits their needs, including making additional copies of the Code of Practice available in languages other than English.

This Code is supplemented by Model Procedural Documents also developed by the CCTV User Group which inter-relate with the contents and requirements of this Code and are essential handbook for all managers and operators of CCTV Systems.

This model should be used in addition to any local 'Partnership Agreements' that should exist between your organisation, the local authority or the Police where they are jointly involved in developing, implementing and managing a CCTV system.

Any 'partners' to a CCTV system should all sign and certify their commitment to abide by these codes at all times whilst involved with the scheme. (Appendix O – Certificate of Agreement)

APPENDIX K COMPLAINTS PROCEDURE

Signage displayed in public areas indicates the contact point for any complaints.

Persons should be made aware that:-

a) All complaints must be made in writing to the CCTV Manager, Devizes Development Partnership, The Crown Cantre, 39 ST John's Street, Devizes SN10 1BL

b) All complaints will be acknowledged in writing within 3 working days and will receive a detailed response within 20 working days

Those persons making a complaint should be provided with on request:-

c) The leaflet which individuals receive when they make a subject access request as general information.

d) A copy of this code.

e) A subject access request form if required or requested.

The CCTV Manager should ensure:-

f) A record of the number of complaints or enquiries should be maintained.

g) A report on those numbers of complaints should be collected by the manager or designated volunteer in order to assess public reaction to, and opinion of, the use of the system.

h) An annual report should be produced which evaluates the effectiveness of the system.

If the complaint cannot be resolved by the CCTV Manager:-

i) the matter will be referred to the DDP Executive Committee for their consideration and response.

All complaints shall be reported to Kennet District Council.

APPENDIX L DEED OF ADHERENCE

APPENDIX M DISCIPLINE CODE

All persons who have contact with the System undertake to adhere to the Code of Practice & Procedural Manual.

Any persons found not to be complying with the same will be removed from having any contact with the System.

APPENDIX N PROCEDURAL MANUAL

Certificate of Agreement

The content of this Code of Practice are hereby approved in respect of Devizes Development Partnership Closed Circuit Television System and, as far 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 Devizes Chamber of Commerce

Signature ……..

Name ……..

Position …….. Dated …….

Signed for and on behalf of Devizes Development Partnership

Signature ……..

Name ……..

Position …….. Dated ……..

Signed for and on behalf of Devizes Town Council

Signature ……..

Name ……..

Position …….. Dated ……..

Signed for and on behalf of Wiltshire Constabulary

Signature ……..

Name ……..

Position …….. Dated …….