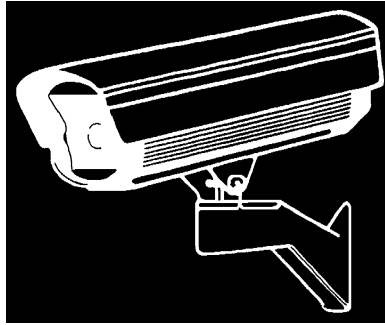


Vale of White Horse

in partnership with

Thames Valley Police

(Southern Oxfordshire Police Area)



Code of Practice

in respect of the operation of

Closed Circuit Television

November 2001



Table of Contents

Preface

Since its introduction to retailers in 1967, the first town centre in 1985 and villages, town and cities throughout the Thames Valley, the use of closed circuit television across the U.K. has become increasingly popular. Arguably, CCTV is one of the most powerful tools to be developed during recent years to assist with effort to combat crime and disorder whilst enhancing community safety. Equally, it may be regarded by some as the most potent infringement of peoples' liberty.

Despite this rapid growth of systems there was, until recently, a dearth of statutory regulation governing the use of CCTV cameras. If we, as users, owners and managers of such systems, are to command the respect of the general public, these systems must not only be used in accordance with current legislation, fairly and lawfully, with the utmost probity at all times. They must also be used in a manner which stands up to scrutiny and is accountable to the very people they are aiming to protect.

Vale of White Horse District Council and Thames Valley Police are committed to the belief that everyone has the right to respect for his or her private and family life and their home. We also believe that there should be no interference by any public body with the exercise of this right except such as may be in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

We are also very aware of the inherent weaknesses if effective control and monitoring procedures are not put in place and followed meticulously. CCTV systems should be operated with respect for all individuals, recognising the right to be free from degrading treatment and avoiding discrimination on any grounds such as sex, race, colour, language, religion, property, birth or other status. Local operating procedures ensure that evidence is secured, retained and made available as required to ensure that there is absolute respect for everyone's right to a fair trial. This Code of Practice complies with the law and, as far as is reasonably practicable, ensures the right to privacy is not breached. It is to be used in addition to the Data Protection Act – Code of Practice for CCTV, which only provides standards to be met to ensure compliance with that Act.

We acknowledge the guidance of the National CCTV User Group and their Standards Committee from the publication of their 'model documents', together with the Oxford City Centre CCTV System Manager and the Thames Valley Police Human Rights Audit Team. The collective work by those involved has greatly assisted the preparation of this document.

Whilst the content of this Code of Practice is accurate at the time of origination, differences and alteration to laws of evidence and procedural matters will inevitably arise. The content of this document is not intended to form a contract. Neither Vale of White Horse District Council nor Thames Valley Police can accept liability for any error or omission or for the advice, guidance or information contained herein.

Code of Practice
in respect of the operation of
Closed Circuit Television

in

The Vale and South Oxfordshire

between
Vale of White Horse District Council
And
Thames Valley Police

Certificate of Agreement

The content of both this Code of Practice its associate Procedural Manual are hereby approved in respect of the Wycombe & Chiltern Closed Circuit Television Systems and, as far as is reasonably practicable, will be complied with by all who are involved in the management and operation of the System.

Approved on behalf of *Vale of White Horse District Council*

Name: Terry Stock

Position held: Chief Executive

Approved on behalf of *Thames Valley Police*

Name: Philip Gormley

Position held: Area Commander (Southern Oxfordshire Area)

Dated the 24th day of December 2001

Section 1 Introduction and Objectives

1.1 Introduction

- 1.1.1 Closed Circuit Television (CCTV) systems have been introduced to the Vale of White Horse District. These systems, known as 'The Vale and South Oxfordshire CCTV System', comprise a number of cameras installed at strategic locations. Some 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. Secondary monitoring facilities are located at police control rooms but there are no recording facilities at any location other than the CCTV monitoring room.
- 1.1.2 The CCTV Systems have evolved from the formation of a partnership between:
- Thames Valley Police
 - Thames Valley Partnership for Safer Communities
 - Abingdon Town Council
 - Wantage Town Council
 - Abingdon Chamber of Commerce
 - Vale of White Horse District Council
 - Businesses in Abingdon and Wantage who are not Members of the respective Chamber of Trade who have pledged financial support
 - South Oxfordshire District Council, town councils and businesses in South Oxfordshire district.
- 1.1.3 For the purposes of this document, the joint 'owners' of the system are Vale of White Horse District Council and South Oxfordshire District Council. The System Manager is the Vale of White Horse District Council CCTV/Neighbourhood Warden Manager. Details of key personnel, their responsibilities and contact points are shown at Appendix A to this Code.
- 1.1.4 The use of CCTV in the Vale and South Oxfordshire is considered a necessary and suitable tool to help achieve a reduction in crime, reduce the fear of crime and improve public safety. This assessment is evidenced by an agreed operational requirement document, supported by public consultation. 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 purpose of crime prevention or victim welfare and is also considered a necessary initiative by the partnership towards their duty under the Crime and Disorder Act 1998.
- 1.1.5 For the purposes of the Data Protection Act 1998, the Vale of White Horse District Council and Thames Valley Police are joint data controllers.

2 Objectives of the System

- 1.2.1 The scheme partners have stated the objectives of the CCTV System as being, for example, but not limited to:
- *To help reduce the fear of crime, vandalism and disorder*
 - *To help deter crime, vandalism and disorder*
 - *To secure a safer environment for the citizens of the Vale of White Horse and South Oxfordshire*
 - *To assist the Local Authorities in discharging their duties.*
- 1.2.2 Within this broad outline, the Thames Valley Police Chiltern Vale Area commander, in partnership with the local authorities Chief Executives, may, after consultation, draw up specific objectives based on local concerns. These objectives will be reviewed annually.

- 1.2.3 ~~It is recognised that the scheme may infringe on the privacy of individuals. The scheme will always comply with relevant legislation, to ensure its legality and legitimacy. The scheme shall be used as a~~ proportional response to identified problems and shall only be used in so far as 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 and morals or for the protection of the rights and freedoms of others.
- 1.2.4 The Code of Practice and operational procedures shall ensure that evidence is secured, retained and made available as required to ensure that there is absolute respect for everyone's right to a fair trial.
- 1.2.5 The scheme shall be operated with respect for all individuals, recognising the right to be free from inhuman or degrading treatment, and avoiding discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

1.3 Procedural Manual

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 CCTV system are realised, the procedural manual is based and expands upon the contents of this Code of Practice.

Section 2 Statement of Purpose and Principles

2.1 Purpose

The purpose of this document is to state the intention of the owners and the managers, on behalf of the partnership as a whole and, as far as is reasonably practicable, to support the objectives of The Vale and South Oxfordshire CCTV System (hereafter referred to as 'The System') and to outline how it is intended to do so.

2.2 General Principles

- 2.2.1 The system will be operated in accordance with all the requirements and the principles of the Human Rights Act 1998 and, when appropriate, authorisation for 'directed' surveillance or crime-trend ('Hotspot') surveillance will be obtained in accordance with the Regulation of Investigatory Powers Act 2000 and Thames Valley Police force policy. The system shall be operated in accordance with the Data Protection Act 1998 at all times.
- 2.2.2 The System will be operated fairly, within the law, and only for the purposes for which it was established or which are subsequently agreed in accordance with this Code of Practice.
- 2.2.3 The public interest in the operation of system will be recognised by ensuring the security and integrity of operation procedures.
- 2.2.4 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.
- 2.2.5 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 Cameras and Area of Coverage

- 2.3.1 the areas covered by CCTV to which this Code of Practice refers are the public areas within the responsibility of the operating partners. 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.
- 2.3.2 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.
- 2.3.3 None of the cameras forming part of the System will be installed in a covert manner. Some may be in all-weather domes to satisfy local planning requirements and all cameras are strategically sited to fulfil the operational requirements of the System.

2.4 Monitoring and Recording Facilities

- 2.4.1 A staffed monitoring room is located at Abingdon police station. The CCTV equipment has the capability of recording all cameras simultaneously throughout every 24 hour period
- 2.4.2 Secondary monitoring equipment is located in South Oxfordshire Police Area Control Rooms. No equipment, other than that housed within the main CCTV control room is capable of recording images from any of the cameras. The equipment will only be operated by trained and authorised users.
- 2.4.3 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.

2.5 Human Resources

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

2.5.2 All operators shall receive training relevant to their legal obligations and roles, particularly in respect of 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.

2.6 Processing and Handling of Recorded Material

2.6.1 All recorded material, whether recorded digitally, in analogue format or as a hard copy video print, will be processed and handled strictly in accordance with this Code of Practice and its associated procedures.

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 the Procedural Manual

2.9.1 Any major changes to either the Code of Practice or the Procedural Manual, (i.e. such as will have a significant impact upon the Code of Practice or upon the operation of the system), will take place only after consultation with, and upon the agreement of all organisations with a participatory role in the operation of the system.

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 manager and the owners of The System.

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.

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

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

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 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.

3.2 Data Protection Legislation

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

3.2.2 The 'data controllers' for The System are the Chief Executive of the Vale of White Horse District Council and the Chief Constable of Thames Valley Police. Day to day responsibility for the data is devolved to the System Manager.

3.2.3 All data will be processed in accordance with the principles of the Data Protection Act, 1998 which, in summarised form, includes, but is not limited to:

- i) All personal data will be obtained and processed fairly and lawfully.
- ii) Personal data will be held only for the purposes specified.
- iii) Personal data will be used only for the purposes, and disclosed only to the people, shown within these codes of practice.
- iv) Only personal data will be held which are adequate, relevant and not excessive in relation to the purpose for which the data are held.
- v) Steps will be taken to ensure that personal data are accurate and where necessary, kept up to date.
- vi) Personal data will be held for no longer than is necessary.
- vii) Individuals will be allowed access to information held about them and, where appropriate, permitted to correct or erase it.

3.2.4 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.

3.3 Request for information (subject access)

- 3.3.1 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 data controller.
- 3.3.2 The principles of Sections 7 and 8 of the Data Protection Act 1998 (Rights of Data Subjects and Others) shall be followed in respect of every request. Those Sections are reproduced as Appendix B to these codes.
- 3.3.3 If the request cannot be satisfied 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.
- 3.3.4 The person making a request must be able to satisfactorily prove their identity and provide sufficient information to enable the data to be located.

3.4 Exemptions to the Provision of Information

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

- 3.4.1 Personal data processed for the purpose of
- i) the prevention or detection of crime or
 - 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.

3.5 Criminal Procedures and Investigations Act, 1996

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

Section 4 Accountability and Public Information

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 manager of The System.
- 4.1.2 Cameras will not be used to look into private residential property. Where the equipment permits it 'Privacy zones' may be programmed into the system as required in order to ensure that the inside of any private residential property within range of the system is not surveyed by the cameras. Alternatively, physical measures may be taken to achieve the same result. In any event, 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 System Manager's office. All complaints shall be dealt with in accordance with the Vale of White Horse District Council complaints procedure, a copy of which may be obtained from Vale of White Horse District Council offices. Any performance issues identified will be considered under the organisations disciplinary procedures to which all Vale of White Horse District Council staff, including CCTV personnel, are subject.
- 4.1.4 All CCTV staff are contractually subject to regulations governing confidentiality and discipline. An individual who suffers damage or distress by reason of any contravention of this Code of Practice may be entitled to compensation.

4.2 System Owner

- 4.2.1 The Community Safety Manager, named at Appendix A, being the nominated representative of the system owners, will have unrestricted personal access to the CCTV monitoring room and will be responsible for receiving regular and frequent reports from the manager of the system.
- 4.2.2 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 nominated 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 Vale of White Horse District Council's head of Audit (or nominated deputy whose organisational level of responsibility is at least equal to that of the System Manager, but who is not the System Manager).
- 4.3.3 The System Manager will ensure that every complaint is acknowledged in writing within five working days. The acknowledgment will include advice to the complainant of the enquiry procedure to be undertaken. A formal report will be forwarded to the nominee of the system owner, named at Appendix A. The report will give details of all complaints and the outcome of relevant enquiries.
- 4.3.4 The System owners shall be informally notified within seven working days of any complaints.
- 4.3.5 Statistical and other relevant information, including any complaints made, will be included in the Annual Reports of Vale of White Horse District Council, which are made publicly available.

4.4 Public Information

4.4.1 Code of Practice

A copy of this Code of Practice shall be published on Vale of White Horse District Council's web site and a copy will be made available to anyone on request. Additional copies will be lodged at public libraries, police stations and Vale of White Horse District Council offices.

- 4.4.2 A small informative leaflet summarising this Code of Practice and containing information on the complaints procedure and subject access requests shall also be available from the same offices.

4.4.3 Signs

Signs (similar to that shown below) will be placed in the locality of the cameras and at main entrance points to the relevant areas, e.g. Railway and Bus stations. 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 above nationally recognised sign, developed by The CCTV User Group, has been adopted as it 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 Office of the Information Commissioner and the Police Scientific Development Branch of the Home Office have also assessed the sign.

Section 5 Assessment of the System and Code of Practice

5.1 Evaluation

5.1.1 The System will periodically be professionally 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 business*
- 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 outcome of the evaluation will be published in summary form in the Annual Report 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.

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

5.2 Monitoring

- ~~5.2.1 The System Manager is responsible for the monitoring and operation of the system and for ensuring compliance with this Code of Practice.~~
- 5.2.2 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

5.3.1 The Vale of White Horse District Council Head of Audit, or his/her nominated deputy, who is not the System Manager, will be responsible for regularly auditing the operation of the system and the compliance with this Code of Practice. Audits, which may be in the form of irregular spot checks, will include examination of the monitoring room records, recording histories and the content of recorded material.

Section 6 Human Resources

6.1 *Staffing of the Monitoring Room and those responsible for the operation of The System.*

- 6.1.1 The CCTV Monitoring Room will be staffed in accordance with the procedural manual. Only authorised personnel who have been properly trained in all monitoring room procedures and its use will operate equipment associated with The System.
- 6.1.1 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. They will be required to sign a confirmation that they fully understand the obligations that adherence to these documents places upon them and that any breach will be considered as 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 as far as is reasonably practicable at all times.
- 6.1.2 Arrangement may be made for a police liaison officer to be present in the monitoring room at certain times, or indeed at all times, subject to locally agreed protocols. Any such person must also be conversant with this Code of Practice and associated Procedural Manual.
- 6.1.3 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*

- 6.2.1 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 discipline code. Any breach of this Code of Practice or of any aspect of confidentiality will be dealt with in accordance with those discipline rules.
- 6.2.2 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 has day to day responsibility for the management of the room and for enforcing the discipline rules. Non-compliance with this Code of Practice by any person will be considered a severe breach of discipline and dealt with accordingly including, if appropriate, the instigation of criminal proceedings.

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 Section 8 concerning access to the monitoring room by others).

Section 7 Control and Operation of Cameras

7.1 Guiding Principles

- 7.1.1 Any person operating the cameras will act with utmost probity at all times.
- 7.1.2 The cameras, control equipment, recording and reviewing equipment shall at all times only be operated by persons who have been trained in their use and the legislative implications of their use.
- 7.1.2 Every use of the cameras will accord with the purposes and key objectives of the system and shall be in compliance with this Code of Practice.
- 7.1.3 Cameras will not be used to look into private residential property. 'Privacy zones' may be programmed into the system or physical measures taken (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.
- 7.1.4 Camera operators will be mindful of exercising prejudices, which may lead to complaints of the system being used for purposes other than those for which it is intended. 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

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

7.3 Secondary Monitoring

- 7.3.1 No secondary control or recording facilities are installed.
- 7.3.2 Secondary monitoring facilities are provided at Thames Valley police control rooms.

The use of secondary 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

- 7.4.1 Under extreme circumstances the Police may make a request to assume direction of The System. Only requests made on the written authority of a police officer not below the rank of Superintendent will be considered. Any such request will only be accommodated on the personal written authority of the most senior representative of the owners of The System, or designated deputy of equal standing.
- 7.4.2 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.
- 7.4.3 In very extreme circumstances a request may be made for 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 System 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 equivalent in standing to the rank of Assistant Chief Constable. The System owners will authenticate all such requests.

~~7.4.4 Should this occur, Thames valley Police accept full liability for any and all acts omissions and failures and agree to fully indemnify the Vale of White Horse District Council for all such liabilities.~~

7.5 Maintenance of the system

- 7.5.1 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 under a maintenance agreement.
- 7.5.2 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.
- 7.5.3 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.
- 7.5.4 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.
- 7.5.5 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.
- 7.5.6 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.

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 into the scope of the above paragraph and may take place at any time, without prior warning. Any visit will be suspended in the event of it being operationally necessary. All visits shall 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 will be required to sign the visitors book and a declaration of confidentiality.

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, 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.

The monitoring room will at all times be secured 'digi-Locks' requiring an alpha numeric code for entrance or other equally secure means.

Section 9 Management Data, including Recorded Material

9.1 Guiding Principles

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

9.1.2 Every recording obtained by using The System has the potential of containing material that has to be admitted in evidence at some point during its life span.

9.1.3 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.

- 9.1.4 ~~It is therefore of the utmost importance that all data obtained from, or used in conjunction with, the system 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.~~
- 9.1.5 Access to and the use of data will be strictly for the purposes defined in this Code of Practice only.
- 9.1.6 Recorded material will not be copied, sold, otherwise released or used for commercial purposes or for the provision of entertainment.

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

- 9.2.1 Every request for the release of personal data generated by this CCTV System will be channelled through the System Manager. The System Manager will ensure the principles contained within Appendix C to this Code of Practice are followed at all times.
- 9.2.2 In complying with the national standard for the release of data to third parties, it is intended, as far as reasonably practicable, to safeguard the individual's rights to privacy and to give effect to the following principles:

- Recorded material shall be processed lawfully and fairly, and used only for the purposes defined in 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;

- 9.2.3 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 data (in whatever format) which may be part of a current investigation, would be covered by the Police and Criminal Evidence Act, 1984. Any such disclosure shall only be made by the police officer in charge of the case.

- 9.2.4 If material is to be shown to witnesses, including police officers, for the purpose of obtaining identification evidence, it must be shown in accordance with Appendix C and the Procedural Manual.
- 9.2.5 It may be beneficial to make use of 'real' video footage for the training and education of those involved in the operation and management of CCTV systems, and for those involved in the investigation, prevention and detection of crime. Any material recorded by virtue of this CCTV system will only be used for such bona fide training and education purposes. Recorded material will not be released for commercial or entertainment purposes.

9.3 **Recording Media - Provision & Quality**

- 9.3.1 To ensure the quality of recorded data and that recorded information will meet the criteria outlined by current Home Office guidelines, the media to be used with the system are those which have been specifically provided in accordance with the Procedural Manual.

9.4 **Control and Management of Media**

- 9.4.1 Media will be used in accordance with the Procedural Manual at all times.
- 9.4.2 All removable media will have a unique tracking record.
- 9.4.3 All media shall be destroyed at the end of their operational life. Such destruction shall be in accordance with the Procedure Manual and the destruction shall be certified. Tracking records shall, however, be retained for a further three years after the media has been destroyed.

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

Section 10 Video Prints

10.1 *Guiding Principles*

- 10.1.1 A video print is a copy of an image or images which already exist on videotape / computer disc. Such prints are equally within the definitions of 'data' and recorded material.
- 10.1.2 Video prints will not be taken as a matter of routine. Each time a print is made it must be capable of justification by the operator who will be responsible for recording the full circumstances under which the print is taken in accordance with the Procedural Manual.
- 10.1.3 Video prints contain data and will therefore only be released under the terms of Appendix C to this 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.
- 10.1.4 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.
- 10.1.5 The records of the video prints taken will be subject to audit in common with all other records in the system.

Key Personnel and Responsibilities

A.1 Ownership

The owner of the System is:

Vale of White Horse District Council
The Abbey House
Abingdon
Oxfordshire OX14 3JE

Tel: 01235 520202

The Community Safety Manager, Mr Bill Jones, telephone number 01235 540309, will be the single point of reference on behalf of the owners.

A.1.1 Responsibilities:

The owners' representative's role includes a responsibility to:

- Maintain close liaison with the control room manager.
- Ensure the interests of the joint owners and other organisations are upheld in accordance with the terms of this Code of Practice.
- In partnership with the system manager, agree to any proposed alterations and additions to the system, this Code of Practice and / or the Procedural Manual.

A.2 System Management

The System manager is:

Mr M Batchelor
CCTV Control
Thames Valley Police
Colwell Drive
Abingdon OX14 1AU

Tel: 01235 556929

A.2.1 Responsibilities:

The System manager has responsibility as 'data manager' to exercise day-to-day control of data on behalf of the data controller. His role includes a responsibility to:

- Maintain day to day management of the system and staff;
- Ensure the provision and maintenance of all equipment forming part of the Vale of White Horse District Council's CCTV System in accordance with contractual arrangements which the owners may from time to time enter into;
- Accept overall responsibility for the system and for ensuring that this Code of Practice is complied with;
- Maintain direct liaison with the owners of the system.
- Maintain direct liaison with operating partners.

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

- (5) In subsection (4) the reference to information relating to another individual includes a ~~reference to information identifying that individual as the source of the information sought by~~ the request; and that subsection is not to be construed as excusing the data controller from communicating so much of the information sought by the request as can be communicated without disclosing the identity of the other individual concerned, whether by omission of names or other identifying particulars or otherwise.
- (6) In determining for the purposes of subsection (4)(b) whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned, regard shall be had, in particular, to:
- (a) any duty of confidentiality owed to the other individual,
 - (b) any steps taken by the data controller with a view to seeking the consent of the other individual,
 - (c) whether the other individual is capable of giving consent, and
 - (d) any express refusal of consent by the other individual.

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 may be prescribed;

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

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

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:**

<http://www.dataprotection.gov.uk/>

Section 8

- ~~(1) The Secretary of State may by regulations provide that, in such cases as may be prescribed, a request for information under any provision of subsection (1) of section 7 is to be treated as extending also to information under other provisions of that subsection.~~
- (2) The obligation imposed by section 7(1)(c)(i) must be complied with by supplying the data subject with a copy of the information in permanent form unless:
- (a) the supply of such a copy is not possible or would involve disproportionate effort, or
 - (b) the data subject agrees otherwise;
 - (c) and where any of the information referred to in section 7(1)(c)(i) is expressed in terms which are not intelligible without explanation the copy must be accompanied by an explanation of those terms.
- (3) Where a data controller has previously complied with a request made under section 7 by an individual, the data controller is not obliged to comply with a subsequent identical or similar request under that section by that individual unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request.
- (4) In determining for the purposes of subsection (3) whether requests under section 7 are made at reasonable intervals, regard shall be had to the nature of the data, the purpose for which the data are processed and the frequency with which the data are altered.
- (5) Section 7(1)(d) is not to be regarded as requiring the provision of information as to the logic involved in decision-taking if, and to the extent that, the information constitutes a trade secret.
- (6) The information to be supplied pursuant to request under section 7 must be supplied by reference to the data in question at the time when the request is received, except that it may take account of any amendment or deletion made between that time and the time when the information is supplied, being an amendment or deletion that would have been made regardless of the receipt of the request.
- (7) For the purposes of section 7(4) and (5) another individual can be identified from the information being disclosed if he/she can be identified from that information, or from that and any other information which, in the reasonable belief of the data controller, is likely to be in, or to come into, the possession of the data subject making the request.

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:**

<http://www.dataprotection.gov.uk/>

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.

The System owners and operating partners are committed to the belief that everyone has the right to respect for his or her private and family life and their home. Although the use of CCTV cameras has become widely accepted in the UK as an effective security tool, those people who do express concern tend to do so over the handling of the information (data) 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 Procedure Manual. All such requests shall be channelled through the data controller.

3. Primary Request To View Data

- a) Primary requests to view data generated by a CCTV System are likely to be made by third parties for any one or more of the following purposes:
 - i) Providing evidence in criminal proceedings (e.g. Police and Criminal Evidence Act 1984, Criminal Procedures & Investigations Act 1996, etc.);
 - ii) Providing evidence in civil proceedings or tribunals
 - iii) The prevention of crime
 - iv) The investigation and detection of crime (may include identification of offenders)
 - v) Identification of witnesses
- b) Third parties, which are required to show adequate grounds for disclosure of data within the above criteria, may include, but are not limited to:
 - i) Police ⁽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⁾
 - iii) Other agencies, (which should be specified in the Code of Practice) according to purpose and legal status⁽⁴⁾.
- c) Upon receipt from a third party of a bona fide request for the release of data, the 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 be restricted to the civil police but could include, (for example) British Transport Police, Ministry of Defence Police, Military Police, etc. (It may be appropriate to put in place special arrangements in response to local requirements).
- (2) Aside from criminal investigations, data may be of evidential value in respect of civil proceedings or tribunals. In such cases a solicitor, or authorised representative of the tribunal, 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 investigation. 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)

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.

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 public well being
 - ii) identifies a public health or safety issue
 - iii) leads to the prevention of crime
- (2) The disclosure of personal data which is the subject of a 'live' criminal investigation would always come under the terms of a primary request, (see III above).

4. 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;
 - iv) 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 requestor 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 other personal data, then the material shall be sent to an editing house for processing prior to being sent to the requestor.

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

7. Media disclosure

Set procedures for release of data to a third party should be followed, If the means of editing out o

- a) In the event of a request from the media for access to recorded material, the procedures outlined under 'secondary request to view data' shall be followed. If material is to be released the following procedures shall be adopted:
- i) The release of the material must be accompanied by a signed release document that clearly states what the data will be used for and sets out the limits on its use.
 - ii) The release form shall state that the receiver must process the data in a manner prescribed by the data controller, e.g. specific identities/data that must not be revealed.
 - iii) It shall require that proof of any editing must be passed back to the data controller, either for approval or final consent, prior to its intended use by the media (protecting the position of the data controller who would be responsible for any infringement of Data Protection legislation and the 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.*

Attention is drawn the requirements of the Information Commissioners in this respect detailed in her 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.

Data Subject Access Request Form

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. Vale of White Horse District Council will only give that information if it is satisfied as to your identity. If release of the information will disclose information relating to another individual(s), who can be identified from that information, the Council is not obliged to comply with an access request unless –

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

Vale of White Horse District Council's Rights

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

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

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

Fee

A fee of £10 is payable for each access request, which must be in pounds sterling. Cheques, Postal Orders, etc. should be made payable to **Vale of White Horse District Council**.

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

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

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

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

Section 4 You must sign the declaration

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

THE CCTV CONTROL ROOM MANAGER,
Thames Valley Police Station, Colwell Drive, Abingdon, OX11 5AU
or take it to any main Vale of White Horse District Council building.
(Receptionist – please complete 'Official Use' Section on page 5).

**If you have any queries regarding this form, or your application, please ring
the CCTV Manager on (01235) 556929**

SECTION 1 About Yourself

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

PLEASE USE BLOCK LETTERS

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

Your Current Home Address (to which we will reply)	
	<i>PostCode</i>
<i>A telephone number will be helpful in case you need to be contacted.</i>	<i>Tel. No.</i>

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

Previous address(es)		
Dates of occupancy	<i>From:</i>	<i>To:</i>
Dates of occupancy	<i>From:</i>	<i>To:</i>

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	<input type="checkbox"/>
-----	--------------------------

(b) Only view the information

YES	<input type="checkbox"/>
-----	--------------------------

SECTION 4 Declaration

DECLARATION (to be signed by the applicant)

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

Signed by

Date

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

NOW – please complete Section 5 and then check the ‘CHECK’ box (on page 5) 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 the relevant section overleaf.

Were you: (tick box below)

<i>A person reporting an offence or incident</i>	<input type="checkbox"/>
<i>A witness to an offence or incident</i>	<input type="checkbox"/>
<i>A victim of an offence</i>	<input type="checkbox"/>
<i>A person accused or convicted of an offence</i>	<input type="checkbox"/>

<i>Other – please explain</i>	

<i>Date(s) and time(s) of incident</i>	
<i>Place incident happened</i>	
<i>Brief details of incident</i>	

Before returning this form • Have you completed ALL Sections in this form?

Please check:

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

Further Information:

These notes are only a guide. The law is set out in the Data Protection Act, 1998, obtainable from The Stationery Office. Further information and advice may be obtained from: **The Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Tel. (01625) 545745**

Please note that this application for access to information must be made direct to **THE CCTV CONTROL ROOM MANAGER, Thames Valley Police Station, Colwell Drive, Abingdon, Oxfordshire, OX11 5AU** and **NOT** to the Data Protection Commissioner.

OFFICIAL USE ONLY

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

Application checked and legible?

Date Application Received

Identification documents checked? Fee Paid

Details of 2 Documents (see page 3)

Method of Payment Receipt No.

Documents Returned?

Member of Staff completing this Section:

Name Location

Signature Date

**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 came into force on 2nd October last. It relates to surveillance by the Police and other agencies and deals in part with the use of directed covert surveillance. Section 26 of this act sets out what is Directed Surveillance. It defines this type of surveillance as:-

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

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

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 sub section **c** above, i.e. it will be an immediate response to events or circumstances. In this case, it would not require authorisation unless it were to continue for some time. 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 required.

Slow time requests are authorised by a Superintendent or above.

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

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

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

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

This should include the name of the officer authorising.

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

Examples:

Insp. 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.

Supt 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 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. It should be used in addition to the Data Protection Act - Code of Practice for CCTV which only provides standards to be met to ensure compliance with that act.

In developing these Codes of Practice we acknowledge the guidance and assistance of a great many organisations and Local Authorities throughout the UK but particularly mention the assistance of Thames Valley Police and their Human Rights Audit Team. The collective work by all the individuals and organisations involved has greatly assisted in the preparation of this document and makes it, we believe the foremost point of reference in developing that essential Code of Practice which is critical for any CCTV system.

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 the 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 the 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.

The installation of any disk version of this document or any download from the internet is undertaken entirely at the risk of the individual user

Whilst the content of this document is thought to be accurate at the time of origination, differences and alterations to laws of evidence and procedural matters will inevitably arise. The content of the document is not intended to form a contract. Neither The CCTV User Group, the officers of the group, the members of the Standards Committee or the members of The CCTV User Group can accept liability for any error or omission or for the advice, guidance or information contained within the Model Codes of Practice.