



Runnymede Borough Council

in partnership with

Spelthorne Borough Council,
Elmbridge Borough Council,
Epsom & Ewell Borough Council,
Ashford St Peter's Hospitals NHS Trust,
Sir William Perkins's School,
Thorpe Park and Surrey Police.

Code of Practice

for the operation of
Closed Circuit Television
based upon



Model Documents (2001)
Amended to comply with the guidance
Of The Information Commissioner
(2008)

April 2012

Safer Runnymede Code of Practice – April 2012
Based upon The CCTV User Group Model Code of Practice © Copyright

Section 1 Introduction and Objectives

1.1 Introduction

A Closed Circuit Television (CCTV) system has been introduced to *Runnymede, Partner Boroughs and other Organisations*. This system, known as the 'Safer Runnymede' system, comprises a number of cameras installed at strategic locations. Most 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 and control facilities are located at the private premises of *St Peter's Hospital and Thorpe Park* where there is recording equipment for cameras located on the local sites only.

The 'Safer Runnymede' CCTV System has evolved from the formation of a partnerships between *Runnymede Borough Council, Spelthorne Borough Council, Ashford St Peter's Hospitals NHS Trust, Thorpe Park, Sir William Perkins School, Elmbridge Borough Council, Epsom & Ewell Borough Council and Surrey Police* who have all acknowledged the Safer Runnymede Code of Practice.

For the purposes of this document, the 'owner' of the system is Runnymede Borough Council but cameras may belong to partners. **For the purposes of the Data Protection Act the 'data controller' is Runnymede Borough Council.**

The 'system manager' is Runnymede Borough Council.

The CCTV system has been notified to the Information Commissioner.

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

*Note1. The **data controller** is the person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are to be processed. It must be a legal entity, e.g. person, organisation or corporate body and in the case of partnerships all partners may be considered to bear the responsibility.*

1.2 Partnership Statement in respect of The Human Rights Act 2003

1.2.1 The Partnership recognises that public authorities and those organisations carrying of the functions of a public service nature are required to observe the obligations imposed by the Human Rights Act 2003, and consider that the use of CCTV in Runnymede and in partners organisations is a necessary, proportionate and suitable tool to help reduce crime, reduce the fear of crime and improve public safety.

1.3 Partnership Statement in respect of The Human Rights Act 2003

1.3.1 The Partnership recognises that public authorities and those organisations carrying of the functions of a public service nature are required to observe the obligations imposed by the Human Rights Act 2003, and consider that the use of CCTV in Runnymede and in partners organisations is a necessary, proportionate and suitable tool to help reduce crime, reduce the fear of crime and improve public safety.

- 1.3.2 This assessment is evidenced by an agreed 'operational requirement' document and public survey. Section 163 of the Criminal Justice and Public Order Act 1994 creates the power for local authorities to provide closed circuit television coverage of any land within their area for the purposes of crime prevention or victim welfare and it is also considered a necessary initiative by Runnymede Borough Council, Spelthorne Borough Council, Ashford St Peter's Hospitals NHS Trust, Thorpe Park, Elmbridge Borough Council, Epsom & Ewell Borough Council and Surrey Police towards their duty under the Crime and Disorder Act 2003.
- 1.3.3 It is recognised that operation of the CCTV System may be considered to infringe on the privacy of individuals. The Partnership recognises that it is their responsibility to ensure that the scheme should always comply with all relevant legislation, to ensure its legality and legitimacy. The scheme will only be used as a proportional response to identified problems and be used only insofar as it is necessary in a democratic society, in the interests of national security, public safety, the economic well being of the area, for the prevention and detection of crime or disorder, for the protection of health and morals, or for the protection of the rights and freedoms of others.
- 1.3.4 The Codes of Practice and observance of the Operational Procedures contained in the manual shall ensure that evidence is secured, retained and made available as required to ensure there is absolute respect for everyone's right to a free trial.
- 1.3.5 The CCTV System shall be operated with respect for all individuals, recognising the right to be free from inhuman or degrading treatment and avoiding discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

1.4 Objectives of the System

- 1.4.1 The objectives of the CCTV System as determined by the Partnership which form the lawful basis for the processing of data are:-
- *To help reduce the fear of crime*
 - *To help deter crime*
 - *To help detect crime and disorder and provide evidential material for court proceedings*
 - *To assist in aspects of town centre and traffic management*
 - *To improve the safety and security of residents, visitors and the business community who use the facilities in the areas covered*
 - *To assist the Local Authority in its enforcement and regulatory functions*
 - *To assist the partners in monitoring and managing their assets*
 - *To assist in supporting civil proceedings which will help detect crime*
 - *To improve public protection*
 - *To enhance generally the environment and thereby improve the facilities for those who use them*

1.5 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. It is not a public document.

Section 2 Statement of Purpose and Principles

2.1 Purpose

- 2.1.1 The purpose of this document is to state the intention of the owners and the managers, on behalf of the Partnership as a whole and as far as is reasonably practicable, to support the objectives of *the CCTV System* (hereafter referred to as 'the System') and to outline how it is intended to do so.
- 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 Act 2003.
- 2.2.2 The operation of the System will also recognise the need for formal authorisation of any covert 'Directed' surveillance or crime trend ('hotspot') surveillance as required by the Regulation of Investigatory Powers Act 2000 and the Police Force Policy.
- 2.2.3 The System will be operated in accordance with the Data Protection Act at all times.
- 2.2.4 The System will be operated fairly, within the law, and only for the purposes for which it was established and are identified within this Code, or which are subsequently agreed in accordance with this Code of Practice.
- 2.2.5 The System will be operated with due regard to the principle that everyone has the right to respect for his or her private and family life and their home.
- 2.2.6 The public interest in the operation of the System will be recognised by ensuring the security and integrity of operational procedures.
- 2.2.7 Throughout 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.
- 2.2.8 Participation in the System by any organisation, individual or authority assumes an agreement by all such participants to comply fully with this Code and to be accountable under the Code of Practice.

2.3 Copyright

- 2.3.1 Copyright and ownership of all material recorded by virtue of the System will remain with the data controller.

2.4 Cameras and Area Coverage

- 2.4.1 The areas covered by CCTV to which this Code of Practice refers are the public areas within the responsibility of the operating partners and cover Addlestone, Chertsey, Egham, Englefield Green, Virginia Water, New Haw, Pooley Green, Ottershaw, Staines, Ashford, Stanwell, Sunbury, Shepperton, St Peter's Hospital, Ashford Hospital, Thorpe Park, Bournewood, Walton, Hersham, Claygate, Long Ditton, Weybridge, West Molesey, Hampton Court, Cobham, Stoneleigh, Ewell, Epsom and Esher.
- 2.4.2 From time to time transportable or mobile cameras may be temporarily sited within the area. The use of such cameras, and the data produced by virtue of their use, will always accord with the objectives of the CCTV System and be governed by these Codes and Procedures.
- 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 the presence of all cameras will be identified by appropriate signs.
- 2.4.5 A map showing the number and location of all fixed cameras in Runnymede is available on the Runnymede Borough Council web site at www.runnymede.gov.uk.

2.5 Monitoring and Recording Facilities

- 2.5.1 A staffed monitoring room is located at the Civic Centre, Station Road, Addlestone. The CCTV equipment has the capability of recording all cameras simultaneously throughout every 24 hour period.
- 2.5.2 No equipment, other than that housed within the Safer Runnymede CCTV Control Room shall be capable of recording images from any of the cameras except St. Peters Hospital cameras which may be recorded within St. Peter's Hospital and Thorpe Park cameras, which are also recorded at Thorpe Park. St. Peter's Hospital and Thorpe Park monitor their own systems, following their own code of practice, to contractual standards.
- 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. All viewing and recording equipment shall only be operated by trained and authorised users.

2.6 Human Resources

- 2.6.1 Unauthorised persons will not have access without an authorised member of staff being present.
- 2.6.2 Specially selected and trained Operators in accordance with the strategy contained within the Procedural Manual shall staff the monitoring room.
- 2.6.3 All Operators shall receive training relevant to their role in the requirements of the Human Rights Act 2003, Data Protection Act 2003, Regulation of Investigatory Powers Act 2000

and the Codes of Practice and Procedures. They will be licensed by The Security Industry Authority. Further training will be provided as necessary.

2.7 Processing and Handling of Recorded Material

2.7.1 All recorded material, whether recorded digitally or as a hard copy video print, will be processed and handled strictly in accordance with this 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 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.

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.

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.

3.1.2 The storage and security of the data will be strictly in accordance with the requirements of the Data Protection Act 2003 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 controller' for the 'System' is Runnymede Borough Council and day-to-day responsibility for the data will be devolved to the Control Centre Operations Manager. The data retained at St Peter's Hospital will be the responsibility of Ashford and St Peter's Hospital Trust. The data retained at Thorpe Park will be the responsibility of Thorpe Park.

3.2.3 All data will be processed in accordance with the principles of the Data Protection Act, 2003 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.
- viii) 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 System Manager or Data Controller or, in respect of St Peter's Hospital, the Hospital Security Manager, in respect of Thorpe Park, the Thorpe Park Operations Manager.
- 3.3.2 The principles of Sections 7 and 8, 10 and 12 of the Data Protection Act 2003 (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 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.
- 3.3.4 Any person making a request must be able to satisfactorily prove their identity and provide sufficient information to enable the data to be located. The appropriate 'Subject Access' request form is included in Appendix 'G'.

3.4 Exemptions to the Provision of Information

- 3.4.1 In considering a request made under the provisions of Section 7 of the Data Protection Act 2003, reference may also be made to Section 29 of the Act which includes, but is not limited to, the following statement:
- 3.4.2 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.

3.5 Criminal Procedures and Investigations Act, 1996

- 3.5.1 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). 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 2003, (known as subject access).

3.6 Patient Confidentiality

3.6.1 The cameras at St Peter's Hospital require special consideration to ensure patient confidentiality is maintained. To achieve this all cameras on this site have been designated by the Security Manager at St Peter's Hospital as being in one of four categories with detailed procedures in the Procedural Manual. The categories are as follows:

- i) Sensitive – Recorded but not monitored and not viewed without express permission of the Chief Executive or an Executive Director of the Trust. The Chief Executive or Executive Director will also liaise with the Trust's Caldicott Guardian in respect of patient confidentiality issues.
- ii) Confidential – Only monitored and recorded at St Peter's Hospital.
- iii) Restricted – Monitored in both Control Rooms but not relayed to Police Monitoring Centre without just cause.
- iv) Public – Monitored and relayed as areas completely open to unrestricted public 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 and the Control Rooms at both St Peter's Hospital and Thorpe Park is restricted in accordance with this Code of Practice. However, in the interest of openness and accountability, anyone wishing to visit the rooms 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 and 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 System Manager's office. All complaints shall be dealt with in accordance with the Partners' Complaint Procedures, a copy of which may be obtained from their offices. Any performance issues identified will be considered under the organisation's disciplinary procedures to which all members of Runnymede Borough Council 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 position of the Manager of the System (not the Monitoring Room Supervisor), 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 Runnymede Borough Council will nominate a Committee with a 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 nominated Manager named at Appendix 'A' will have day-to-day responsibility for the System as a whole with the Security Manager at St Peter's Hospital responsible for activity on that site and the Security Manager at Thorpe Park responsible for activity on that site.
- 4.3.2 The System will be subject to audit by *Runnymede Borough Council Chief Internal Auditor*, (or nominated deputy).
- 4.3.3 The System Manager and the Security Manager as appropriate 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 undertaken. 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.

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

4.4 Public Information

4.4.1 Code of Practice

A copy of this Code of Practice shall be published on the Runnymede Borough Council web site, and a copy will be made available to anyone on request. Additional copies will be lodged at Public Libraries, Police Stations and Partners' Reception Offices.

4.4.2 Annual Report

The 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 Public Libraries, Local Police Stations and offices of the Partners.

4.4.3 Signs

Signs 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.

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

5.1.3 It is intended that evaluations should take place at least annually.

5.2 Monitoring

5.2.1 The System Manager and Security Manager at St Peter's Hospital/Thorpe Park will accept day-to-day responsibility for the monitoring, operation and evaluation of the System and the implementation of this Code of Practice.

5.2.2 The System Manager and Security Manager at St Peter's Hospital/Thorpe Park 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 Chief Internal Auditor, 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, videotape histories and the content of recorded material.

5.4 Incident Reports

5.4.1 All Operators will make records and complete incident forms in respect of all incidents

occurring as detailed in the Procedural Manual.

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. Equipment associated with the System will only be operated by authorised personnel who will have been properly trained in its use and all monitoring room procedures. All Operators must hold a valid Public Space Surveillance (CCTV) Licence issued by The Security Industry Authority.
- 6.1.2 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 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.
- 6.1.3 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.
- 6.1.4 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 discipline code of their employer. 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/she 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.
- 6.2.3 Declaration of Confidentiality

Every individual with any responsibility under the terms of this Code of Practice and who has any involvement with The System to which they refer, will be required to sign a declaration of confidentiality. (See example at Appendix 'E', see also 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.
- 7.1.3 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.
- 7.1.4 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.
- 7.1.5 Camera operators will be mindful of exercising prejudices, which may lead to complaints of the System being used for purposes other than those for which it is intended. The Operators may be required to justify their interest in, or recording of, any particular individual, group of individuals or property at any time by virtue of the audit of the System or by the System Manager.

7.2 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 at the Safer Runnymede Centre.
- 7.2.2 At both St Peter's Hospital Control Room and Thorpe Park Control Room, local site operators have primacy of control at all times.

7.3 Secondary Control

- 7.3.1 Secondary monitoring only facilities are provided at Surrey Police Force Incident Handling Centre and Runnymede Borough Neighbourhood Office.
- 7.3.2 The use of 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 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 or public safety. Such use will provide the Police with a broad overview of events in order to command the incident.
- 7.4.2 Such requests will be viewed separately to the use of the System's cameras with regard to the requirement for an authority for specific types of surveillance under the Regulation of Investigatory Powers Act 2000. See Appendix I.
- 7.4.3 Applications made as at 7.4.1 above will be considered on the written request of a police officer not below the rank of Superintendent. Any such request will only be accommodated upon the personal written permission of the most senior representative of the System owners, or designated deputy of equal standing. In the event of an urgent need, a verbal request of the Senior Officer in charge, and in any case an officer not below the rank of Inspector, will be necessary. This should be followed as soon as practicable within 72 hours by a Superintendent's written request.
- 7.4.4 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 specifically trained 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 request, taking into account their responsibilities under this Code.
- 7.4.5 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 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 not below the rank of Assistant Chief Constable or person of equal standing.

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 relevant Runnymede Borough Council Manager and the Security Managers at St Peter's Hospital and Thorpe Park as appointed 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 Rooms, (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 Declaration of Confidentiality

8.3.1 Regardless of their status, all visitors to the CCTV Monitoring Rooms, including inspectors and auditors, will be required to sign the visitor's book and a declaration of confidentiality.

8.4 Security

8.4.1 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.

8.4.2 The secure area containing the monitoring room will at all times be secured by 'Magnetic-Locks' operated by the CCTV Operator,

Section 9 Management of 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 onto DVD's and including prints.
- 9.1.2 Every digital recording obtained by using the System has the potential of containing material that has to be admitted in evidence at some point during its 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 irrespective of the means or format (e.g. paper copy, DVD, digital hard drive, CD, or any form of electronic processing and storage) of the images obtained from the System, they are treated strictly in accordance with this Code of Practice 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 recorded material 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 or Security Manager at St Peter's Hospital or Thorpe Park as appropriate. 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;
 - the release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

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 recorded information, 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 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 the defence.*

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 Video Discs - Provision & Quality

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

9.4 Recordings – Retention

9.4.1 Recordings will be retained for a period of one calendar month within the arrays of digital hard drives provided. After that time they will be overwritten by new recordings.

9.4.2 If a recording is believed to include evidence to be used in accordance with the authorised purposes of the System the recording will be archived on a separate hard drive to be available for investigation. The recordings will be retained and stored in accordance with the Procedural Manual. At the conclusion of their life within the CCTV System they will be deleted or overwritten.

9.5 Retained Recorded CCTV Footage

9.5.1 Every time a request is made to retain a CCTV recording, an entry will be made in the Evidential CCTV Data Log which will have a unique tracking record maintained in accordance with the Procedural Manual, which will be retained for at least three years. The tracking record shall identify every use and person who has viewed or had access to the recording since the initial archiving.

9.6 Recording Policy

9.6.1 Subject to the equipment functioning correctly, images from every camera within the System will be recorded throughout every 24 hour period at a rate equivalent to at least 6 frames per second. Any images viewed on the Operators' console monitors shall be additionally recorded in real time.

9.7 Evidential Discs

9.7.1 In the event of a recording being required for evidential purposes the procedures outlined in the Procedural Manual will be strictly complied with. A sealed master copy disc and a working copy disc will be prepared. After those discs have been handed to the Investigating Officer against signature no duplicate recordings will be retained.

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 within a digital recording. Such prints are equally within the definitions of 'data' and recorded material.
- 10.1.2 Video prints will not be taken as a matter of routine. Each time a print is made it must be capable of justification by the originator who will be responsible for recording the full circumstances under which the print is taken in accordance with the 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.

Appendix 'A' Key Personnel and Responsibilities

1. System Owners – Safer Runnymede:

Director of Technical Services

Tel: 01932 838383

Runnymede Borough Council

Civic Centre, Station Road, Addlestone, Surrey, KT15 2AH

Responsibilities:

Runnymede Borough Council is the 'owner' of the system. The Control Centre Manager will be the single point of reference on behalf of the owners. His role will include a responsibility to:

- i) Ensure the provision and maintenance of all equipment forming part of the Runnymede Borough Council System in accordance with contractual arrangements, which the owners may from time to time, enter into.
- ii) Maintain close liaison with the Control Room Senior Operators.
- iii) Ensure the interests of the joint owners and other organisations are upheld in accordance with the terms of this Code of Practice.
- iv) Agree to any proposed alterations and additions to the system, this Code of Practice and/or the Procedural Manual.

2. System Management

Control Centre Operations Manager **838383**

Tel. 01932

Civic Centre, Station Road,
Addlestone, Surrey, KT15 2AH

Responsibilities:

The Control Centre Operations Manager is the 'manager' of the Safer Runnymede System.

He has delegated authority for data control on behalf of the 'data controller'.

His role includes responsibility to:

- i) maintain day-to-day management of the system and staff;
- ii) accept overall 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.

3. System Owners – Borough of Spelthorne:

Community Safety Officer

Council Offices, Knowle Green,
Staines, Middlesex, TW18 1XB

Tel: 01784 444226

Responsibilities:

The Borough of Spelthorne has responsibility for all the CCTV equipment within the Borough of Spelthorne. His role will include a responsibility to ensure that this Code of Practice and associated Procedural Document is complied with at all times particular in respect of the use of the mobile camera system.

4. System Owners – St Peter's Hospital:

Director of Clinical & Non-clinical Support Services and Ashford Hospital Director

Ashford Hospital, London Road,
Ashford, Middlesex, TW15 3AA

Tel: 01784 884488

Responsibilities:

Ashford and St Peter's Hospitals Trust has responsibility for all the CCTV equipment on the St Peter's Hospital site. His role will include a responsibility to ensure that this Code of Practice and associated Procedural Document is complied with at all times.

5. System Management - St Peter's Hospital:

The Security Manager

St Peter's Hospital
Guildford Road, Chertsey, Surrey KT16 0PX

Tel: 01932 872000

Responsibilities:

He has delegated authority for data control on behalf of the 'data controller'.

His role includes responsibility to:

- i) Maintain day-to-day management of the system and staff;
- ii) Accept overall 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.

6. System Owners – Thorpe Park

Tel: 01932 577147

The Operations Director

Thorpe Park
Staines Lane,
Chertsey,
Surrey KT16 8PN

Responsibilities:

Thorpe Park has responsibility for all the CCTV equipment on the Thorpe Park site. His role will include a responsibility to ensure that this code of practice and associated procedural document is complied with at all times.

7. System Management – Thorpe Park

The Security Manager

Thorpe Park
Staines Lane,
Chertsey,
Surrey KT16 8PN

Responsibilities:

He has delegated authority for data control on behalf of the 'data controller'.

His role includes responsibility to:

- i) Maintain day-to-day management of the system and staff;
- ii) Accept overall 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.

8. System Owners – Borough of Elmbridge:

Community Safety Partnership Manager

Tel: 01372 474399

Elmbridge Borough Council,
Civic Centre, High Street,
Esher, Surrey KT10 9SD

Responsibilities:

The Borough of Elmbridge has responsibility for all the CCTV equipment within the Borough of Elmbridge. His role will include a responsibility to ensure that this Code of Practice and associated Procedural Document is complied with at all times particular in respect of the use of the mobile camera system.

9. System Owners – Borough of Epsom & Ewell:

Community Safety Partnership Manager

Tel: 01372 732000

Epsom & Ewell Borough Council

Town Hall, The Parade

Epsom

Surrey

KT18 5BY

Responsibilities:

The Borough of Epsom & Ewell has responsibility for all the CCTV equipment within the Borough of Epsom & Ewell. His role will include a responsibility to ensure that this Code of Practice and associated Procedural Document is complied with at all times particular in respect of the use of the mobile camera system.

Appendix B Extracts from Data Protection Act 2003

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.

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.

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.

All the 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⁾
 - vi) 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.
- Note:** A time limit could apply providing reasonable notice was issued to the agent, prior to the destruction of the held data (e.g. a time limit was about to expire).
- 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)

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 2003, Human Rights Act 2003, 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 2003);
 - 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).

5. Individual Subject Access under Data Protection legislation

- 1) Under the terms of Data Protection legislation, individual access to personal data, of which that individual is the data subject, must be permitted providing:
 - i) the request is made in writing;
 - ii) a specified fee is paid for each individual search;
 - iii) the data controller is supplied with sufficient information to satisfy him or 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 herself or himself 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;
 - 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 requester 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 requester.

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 other personal data does not exist on-site, measures should include:

- 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.

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.

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

Appendix 'E' Declaration of Confidentiality

The Safer Runnymede** CCTV System

I,, am retained by *Runnymede Borough Council*** to perform the duty of CCTV Control Room Operator/Senior Operator/Supervisor/Manager*. I have received a copy of the Code of Practice in respect of the operation and management of that CCTV System.

I hereby declare that:

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

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

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

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

Signed: Print Name:

Witness: Position:

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

* *Delete as appropriate.*

***Substitute St Peter's Hospital if appropriate*

Appendix F Subject Access Request Form **

'SAFER RUNNYMEDE' CCTV SYSTEM - Data Protection Act, 2003

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. Runnymede Borough 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)

Runnymede Borough Council Rights

Runnymede Borough 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 '**Runnymede Borough Council**'.

THE APPLICATION : 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 Runnymede Borough 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 OPERATIONS MANAGER, Runnymede Borough Council,
Civic Offices, Station Road, Addlestone, Surrey, KT15 2AH
(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 Telephone No. 01932 838383**

SAFER RUNNYMEDE CCTV SYSTEM (Data Protection Act 2003)

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>

SAFER RUNNYMEDE CCTV SURVEILLANCE SYSTEM
Data Protection Act, 2003

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 by

Date

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

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

SAFER RUNNYMEDE CCTV SURVEILLANCE SYSTEM
Data Protection Act, 2003

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

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

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

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

Were you: (tick box below)

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

Other – please explain	<input type="text"/>
<input type="text"/>	
<input type="text"/>	
<input type="text"/>	

Date(s) and time(s) of incident	<input type="text"/>
Place incident happened	<input type="text"/>
	<input type="text"/>
Brief details of incident	<input type="text"/>
<input type="text"/>	
<input type="text"/>	

SAFER RUNNYMEDE CCTV SYSTEM - Data Protection Act, 2003

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, 2003, 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 **Runnymede Borough Council** (address on Page 1) and **NOT** to the Data Protection Commissioner.

OFFICIAL USE ONLY

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

Application checked and legible?

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
Signature

Location
Date

**** A similar form exists in respect of data held at St Peter's hospital**

Appendix G Use of Mobile CCTV System

Introduction

Mobile Closed Circuit Television (CCTV) Systems may be operated within Runnymede and Partner Boroughs.

Any system that has the capability of linking in to the existing fixed CCTV system will come under the direct control of the Safer Runnymede Control Room.

This code of practice will then apply.

Other systems can operate independently and where installed, they will fall under the governance of the installing authority.

For example, in Spelthorne the mobile system has evolved from the formation of a Partnership between Spelthorne Borough Council, Spelthorne Police, and Spelthorne Housing Association. For the purposes of the Codes of Practice, the 'owner' of the system is Spelthorne borough Council and the key personnel and responsibilities will be as set out in Appendix A of the Code.

Objectives of the system

The partners in Spelthorne have agreed the objectives of the Mobile CCTV System as being a rapid deployment system:

- To enable the partners to respond to the growing public demand for CCTV in areas outside Staines Town Centre and assist in the evaluation of need for permanent systems and/or other preventive measures for use in specific initiatives.
- To assist the police at crime 'hot-spots' particularly auto-crime and crime/disorder in residential housing areas.
- To evaluate and prosecute with individual incidents of crime including racial/homophobic crime.
- To deal with suspected anti-social behaviour.
- To deter crime.
- To assist in the detection of crime.
- To help reduce the fear of crime.

The system will also be available for use by all Council Departments and authorised external agencies, operating under this code.

Privacy and Data Protection

All personal data obtained by virtue of a Mobile CCTV 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 there home. All data will be processed in accordance with the principals of the Data Protection Acts and is summarised in Appendix B of this Code.

Key Operational Requirements

Before the system can be deployed the purpose of observing each area/target must be defined by the Partner requiring deployment, and this will be documented. Where an area is to be observed for more than one purpose this will also be documented.

Potential conflicts of use will be resolved and principles agreed based on the Crime and Disorder Reduction Strategy, local planning needs, and factors such as threat and risk assessments. A structured analysis of the problem and how the Mobile CCTV System can help in the solution is the key operational requirement.

Appendix H Regulation of Investigatory Powers Act Guiding Principles

Introduction

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

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

Background

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

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

The consequences of not obtaining an authorisation under this Part may be, where there is an interference by a public authority with Article 8 rights (invasion of privacy), and there is no other source of authority, that the action is unlawful by virtue of section 6 of the Human Rights Act 2003 (Right to fair trial) and the evidence obtained could be excluded in court under Section 78 Police & Criminal Evidence Act 1978

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

“Covert surveillance” defined

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

Part II - Surveillance types

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

“Intrusive” surveillance

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

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

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

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

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

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

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

“Directed” surveillance

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

The Act says:

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

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

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

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

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

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

Authorisations:

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

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

e.g.:

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

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

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

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

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

The 'authority' must indicate the reasons and should fall within one of the following categories:-

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

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

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

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

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

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

Policing examples:

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

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

Supt. Authorisation – non-urgent request

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

No authorisation required

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

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

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

Appendix 'I' 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

The 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.

These codes are compiled 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 2003 - Code of Practice for CCTV which provides standards to be met to ensure compliance with that act; the Codes of Practice issued under The Criminal Procedures & Investigations Act 1996; Codes – Police & Criminal Evidence Act 1976 and draft codes under Regulation of Investigatory Powers Act 2000. Any court or tribunal will only recognise Codes of Practice issued under specific legislation.

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.