Spelthorne Borough Council

Code of Practice

For the operation of Closed Circuit Television

In accordance with the guidance from the Information Commissioners Office

February 2017

Section 1 Introduction and Objectives

1.1 Introduction

A Closed Circuit Television (CCTV) system has been in place on Spelthorne Borough for several years and is a combination of - live 24/7 monitored cameras and a system of recorded cameras which are not live monitored.

Of the 86 cameras within the borough 37 are live monitored by the control room at Runnymede Borough Council under a specific partnership agreement known as the Safer Runnymede System and their operation governed by their Codes of Practice.

The remaining 49 cameras are recorded on a stand- alone system in the Community Safety Office at Spelthorne Borough Council and images can be retrieved where required.

There are also CCTV systems at the main offices at Knowle Green and at the day centres within the borough.

For the purposes of this document the owner of the system is Spelthorne Borough Council and for the purposes of the Data Protection Act the data controller is Spelthorne Borough Council.

Note 1. 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, eg person, organisation or corporate body and in the case of partnerships all partners may be considered to bear the responsibility.

The system manager is the Community Safety Manager at - Spelthorne Borough Council

The Information Commissioner has been notified of the system

Details, responsibilities and contact points of the principal personnel are shown at Appendix A to this Code

1.2 Statement in respect of The Data Protection Act 2003

1.2.1

Spelthorne Borough Council recognises that public authorities and those organisations carrying out the functions of a public service nature are required to observe the obligations imposed by the Data Protection Act 2003, and consider that the use of CCTV in Spelthorne is a necessary, proportionate and suitable tool to help reduce crime, reduce the fear of crime and improve public safety.

1.3 Statement in respect of The Human Rights Act 2003

1.3.1

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

1.3.2

It is recognised that the operation of a CCTV system may be considered to infringe on the privacy of individuals. Spelthorne Borough Council recognises that it is their responsibility to ensure that the scheme should always comply with the relevant legislation, to ensure its legality and legitimacy. The scheme will only be used as a proportional response to identified problems and only insofar as it is necessary in a democratic society, and in the interests of national security/public safety/economic well - being of the area/prevention and detection of crime/protection of health and morals/protection of the rights and freedom of others.

1.3.3

The Codes of Practice and associated procedures shall ensure that evidence is secured, retained and made available as required to ensure there is absolute respect for and individuals right to a fair trial.

1.3.4

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 for the system as determined by Spelthorne which from 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 improve the safety and security of residents, visitors and the business community who use the facilities in the areas covered
- To assist the Council in its enforcement and regulatory functions
- To assist in supporting civil proceedings which will help detect crime
- To improve public protection
- To enhance the environment generally and thereby improve the facilities for those who use them

1.5 Procedure Manual

1.5.1

This Code of Practice (hereafter referred to as The Code) is supplemented by a separate Procedural Manual which contains 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 the 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 Council as a whole to support the objectives of the CCTV System (hereafter referred to as the system) and to outline how it is intended to do so.

2.2 General Principles of Operation

2.2.1

The System will be operated in accordance with all the requirements and 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 of crime trend (hotspot) surveillance as required by the Regulation of Investigatory Powers Act 2000 and Police policy.

2.2.3

The system will be operated in accordance with the Data Protection Act 2003 at all times.

2.2.4

The system will be operated fairly, within the law, and only for the purpose for which it was established and are identified within 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 practicable, to balance the objectives of the CCTV system with need to safeguard the individuals rights. Every effort has been made throughout the Code to indicate that a formal structure has been put into 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 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 of Ashford, Shepperton, Stanwell and Sunbury, and any other location should a portable system be deployed. The Council Offices, Depot - and outlying Day Centres are also included.

2.4.2

When justified transportable mobile cameras may be temporarily sited within the area. The use of such cameras and data produced will always accord with the objectives of the system and be governed by theses Codes.

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.

2.4.5

None of the cameras forming part of the system will be installed in a covert manner. Some may be enclosed within all - weather domes for aesthetic or operational reasons but the presence of all cameras will be identified by appropriate signs.

2.4.6

A list detailing the number and location of all fixed cameras in Spelthorne is available on the Spelthorne Borough Council web site in the Community Safety Section

2.5 Monitoring and recording facilities

2.5.1

The public sites CCTV equipment is stand alone and located in the Community Safety Office and has the capability of recording all cameras simultaneously 24/7. There are also systems at the Depot and Council Offices which record in the Council Offices. There is a standalone system at the Greeno Centre in Shepperton.

2.5.2

No equipment, other than that housed within the Community Safety Office, or portable encrypted hard drives externally deployed, shall be capable of recording images from any of the cameras, except those located in Council Offices/Depot and Day centres which are stand alone systems located in their management offices. Staff at these centres do not live monitor their systems and follow this code of practice.

2.5.3

CCTV operators are able to produce hard copies of recorded images, replay or copy any pre-recorded data at their discretion and in accordance with the Codes 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 to the CCTV area without an authorised member of staff being present.

2.6.2

Specially selected and trained operators in accordance with the Codes shall staff the recording 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 associated procedures. There is no requirement for them to be licensed by the Security Industry Authority as they do not carry out 'manned guarding' activities.

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 associated procedure 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 Code of Practice and associated procedures

2.9.1

Any major changes to either the Code of Practice or associated practices (ie- that will have a significant impact on Codes or 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 may be agreed between between the manager and the owners of the system.

Section 3 Privacy and Data Protection

3.1 Public Concern

3.1.1

Whilst the majority of the public at large may have become accustomed to being subject to CCTV cameras those who do express concern do so mainly over the issue of processing of the information (data).

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:

- Organisation, adaption or alteration
- Retrieval, consultation or use of the data
- Disclosure of the data by transmission, dissemination or otherwise making available
- Alignment, combination, blocking, erasure or destruction of the 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.

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 Spelthorne Borough Council and day to day responsibility for the data will be devolved to the Community Safety Manager. The data retained by the Day Centres and the Council Offices will be the responsibility of their management teams.

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:

- All personal data will be obtained and processed fairly and lawfully

- Personal data will be held only for the purpose specified
- Personal data will only be used for the purposes, and disclosed only to the people, shown within these codes of practice
- Only personal data will be held which are adequate, relevant and not excessive in relation to the purpose for which the data are held.
- Steps will be taken to ensure that personal data are accurate and where necessary, kept up to date
- Personal data will be held for no longer than is necessary
- Individuals will be allowed access to information held about them and, where appropriate, permitted to correct or erase it
- Procedures will be implemented to put in place security measures to prevent unauthorised or accidental access to, alteration, disclosure, loss or 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 the day Centres or Council Offices, to their managers.

3.3.2

The principles of Sections 7, 8, 10, 12 of the Data Protection Act 2003 (Rights of Data Subjects and Others) shall be followed in respect of every request, those sections are attached at 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.

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:

Personal data processed for the any of the following reasons 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'*

- The prevention and detection of crime
- The apprehension or prosecution of offenders

Note: 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). Disclosure of unused material should not be confused with the obligations placed on the Data Controller by Section & of the Data Protection Act 2003 (known as Subject Access).

Section 4 Accountability and Public Information

4.1 The Public

4.1.1

For reasons of security and confidentiality, access to the CCTV monitoring room in the Community Safety Office is restricted. However in the interest of openness and accountability anyone wishing to visit the room may be permitted to do so, subject to the approval of the System Manager.

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 utilising the complaints procedure on the SBC website. All complaints shall be dealt with in accordance with the Spelthorne Councils Complaint Procedures, a copy of which may be obtained from the Council Website. Any performance issues identified will be considered under the organisations' disciplinary procedures to which all members of the Community Safety team 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 the Code of Practice may be entitled to compensation.

4.2 System Owner

4.2.1

The position of System Manager named at Appendix A being the nominated representative of the system owners will have unrestricted personal access to the Community Safety Office.

4.2.2

Formal consultation will take place between the owners and managers of the system with regard to all aspects of operation including the contents of the Codes of Practice and the Procedural Manual.

4.2.3

Formal consultation will take place between the owners and managers of the system with regard to all aspects of operation including the contents of the Codes of Practice and the Procedural Manual.

4.3 System Manager

4.3.1

The nominated manager at Appendix A will have day to day responsibility for the system as a whole with Day Centre Managers having responsibility for activity on their respective sites.

4.3.2

The system will be subject to audit by Spelthorne Borough Council Internal Auditor (or nominated deputy). Statistical and other relevant information, including any complaints made, will be included in the Annual Reports which will be made publicly available. This will be made available to the Overview & Scrutiny committee for their observations and comment.

4.3.3

The System Manager and 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 sent to the nominee of the system owner at Appendix A giving details of all complaints and the outcome of relevant enquiries.

4.4 Public Information

4.4.1

A copy of this Code of Practice shall be published on the Spelthorne 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

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 report will be made available to anyone requesting it and publically available.

4.4.3

Signs will be placed in the locality of the cameras and at main entrance points to the relevant areas eg Rail and Bus stations. The signs will indicate

- The presence of CCTV monitoring
- The ownership of the system
- Contact numbers of the Data Controller of the system
- Reason why the CCTV is there

Section 5 Assessment of the System and Code of Practice

5.1 Evaluation

5.1.1

The annual audit process will include 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 their Bidding Guidelines, and be based on assessment of the Inputs, Outputs along with the Process and Impact of the scheme:

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

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 Knowle Green/Day Centre Managers will accept day to day responsibility for the reviewing, operation and evaluation of the system and implementation of the Code of Practice.

5.2.2

The System Manager and Day Centre Managers shall also be responsible for maintaining full management information as to the incidents dealt with/recorded as part of the management of the system and for future evaluations.

5.3 Audit

5.3.1

The 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 spot checks, will include examination of the CCTV room records, video recording histories and the content of recorded material.

5.4 Incident Reports

5.4.1

All operators will make records and complete incident logs of all incidents they are requested to review.

Section 6 Human Resources

6.1.1

The CCTV recording and reviewing room will be not be staffed 24/7. The system will only be operated by authorised personnel who will have been properly trained in its use and all CCTV monitoring and reviewing procedures. They do not require a Public Space Surveillance Licence from the SIA as their activities to not constitute manned guarding activity.

6.1.2

Every person involved in the management and operation of the system will be personally issued with a copy of the Codes of Practice and associated procedures, and will be required to sign a confirmation that they fully understand their obligations under them, and that any breach will be considered as a disciplinary offence. They will be fully conversant with the contents of these

documents which may be updated periodically. Operators will be expected to comply with these documents as far as is reasonably practicable at all times.

6.1.3

Arrangements may be made for a Police Liaison Officer to be present in the recording/reviewing room at certain times subject to locally agreed protocols. Any such person must be conversant with this Code of Practice and associated procedures.

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 or of any aspect of confidentiality will be dealt with in accordance with the discipline codes.

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 Community Safety Office and for enforcing the discipline rules. Non-compliance with this Code 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

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

Section 7 Control and Operation of Cameras

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 purpose 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, groups 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 in the Community Safety Office at Spelthorne Borough Council.

7.2.2

At the Day Centres/Council Offices within the Borough local staff will have primacy of control at all times

7.3 Secondary Control

7.3.1

The use of reviewing facilities will be administered and recorded in full accordance with this Code of Practice and associated procedures which 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 circumstances 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 systems' cameras with regard to the requirement for an authority for specific types of surveillance under the Regulation of Investigatory Powers Act 2000. (see Appendix H)

7.4.3

Applications made at 7.4.1 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 from an officer not below the rank of Inspector will be necessary for consideration. This should be followed as soon as practicable and within 72 hours by a Superintendents' written request.

7.4.4

In the event of such a request being permitted, the Community Safety Office will continue to be staffed and equipment operated by those personnel who are specifically trained to do so, and who fall within the terms of Sections 6 and & of this Code. They will be under the command of the police officer designated in the verbal/written request.

7.4.5

In very extreme circumstances a request may be made for the Police to take total control of the system, including staffing the Community Safety office and personal control of all associated equipment, excluding any 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 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 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 that 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 Spelthorne Borough Council Managers and Day Centre Managers to ensure that 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 Recording Room and Equipment

8.1 Authorised Access

8.1.1

Only trained and authorised personnel will operate any of the CCTV equipment located within the Community Safety Office.

8.2 Public Access

8.2.1

Public access to the monitoring and recording facility will be prohibited except for the 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 these Codes of Practice and associated procedures**.**

8.3 Declaration of Confidentiality

8.3.1

Regardless of their status, all visitors to the Community Safety Office, including Inspectors and Auditors, will be required to sign the visitors' 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 Community Safety Office having to be evacuated for safety or security reasons, the Codes of Practice and associated procedures will be complied with.

Section 9 Management of Recorded Material

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 DVDs 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 (eg paper copy, DVD, digital hard drive, CD/USB stick or any form of electronic processing and storage) of the images obtained from the system, they are treated strictly in accordance with this Code and associated procedures from the moment they are received until final destruction.

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 System will be channelled through the system manager or Day Centre Managers. The system manager will ensure the principles contained within Appendix C to this Code 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 individuals' rights to privacy and to give effect to the following principles:

- Recorded materials shall be processed lawfully and fairly, and used only for the purposes defined in this Code
- Access to recorded material will only take place in accordance with the standards outlined in Appendix C and this Code
- 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 of this Code), 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 procedure associated with this Code.

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 purposes of obtaining identification evidence, it must be shown in accordance with Appendix C and the procedures associated with this Code.

9.3 Video Discs – Provision and Quality

9.3.1

To ensure the quality of the discs/USB data sticks, and that recorded information will meet the criteria outlined by the current Home Office guidelines, the only video discs/USB data sticks to be used with the system are those which have been specifically 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/USB Stick to be available for investigation. The recordings will be retained and stored in accordance with the Procedures associated with this Code. 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 procedures associated to this Code, and 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. (this exists in Section 5 of Procedure Manual)

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 shall be additionally recorded in real time (query Spelthorne)

9.7 Evidential Discs

9.7.1

In the event of a recording being required for evidential purposes the procedures associated with this Code will be strictly complied with. A sealed master copy disc and a working copy disc/USB Stick will be prepared. After those discs have been handed to the Investigating Officer against signature no duplicate will be retained.

Section 10 Video Prints

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 procedures associated with this Code.

10.1.3

Video prints contain data and will therefore only be released under the terms of Appendix C to this Code (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 procedures associated with this Code.

10.1.4

A record will be maintained of all video print productions in accordance with the procedures associated with this Code. 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
- Identity of the person requesting the print
- 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

System Owners - Spelthorne Borough Council

Deputy Chief Executive

Spelthorne Borough Council
Council Offices
Knowle Green
Staines upon Thames TW18 1XB

Responsibilities:
Spelthorne Borough Council is the 'owner' of the system. **The Spelthorne Community Safety Manager** will be the single point of reference on behalf of the owners. His/her role will include a responsibility to:
i) Ensure the provision and maintenance of all equipment forming part of the Spelthorne Borough Council System in accordance with contractual arrangements, which the owners may from time to time, enter into.
ii) Maintain close liaison with the system operators and the Safer Runnymede Manager.
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
Spelthorne Borough Council Community Safety Manager *Tel.*

Council Offices
Knowle Green
Staines upon Thames TW18 1XB

Responsibilities*:*
The Community Safety Manager is the 'manager' of the Spelthorne System
He/she has delegated authority for data control on behalf of the 'data controller'.
His/her 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.

Appendix B Extracts from Data Protection Act 2003 Section 7&8

1 Subject to the following provisions of this section and to sections 8 and 9 an individual is entitled:

- to be informed by any data controller whether personal data of which that individual is subject are being processed by or on behalf of that Data Controller;

- if that is the case, to be given by the Data Controller a description of
  (i) the personal data of which that individual is subject
  (ii) the purpose for which they are or are to be processed
  (iii) the recipients or classes of recipients to whom they are or may be disclosed;

- 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 to the source of those data;

- 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 credit worthiness, his/her reliability or his/her conduct, has constituted or is likely to constitute the sole basis of 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:

  (i) A request in writing, and
  (ii) 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:

  (i) The other individual has consented to the disclosure of the information to the person making the request; or
  (ii) It is reasonable in all circumstances to comply with the request without the consent of the other individual

5

- In subsection (4) the reference to information relating to another individual includes a reference to information identifying that individual as the source of 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 purpose 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:

  (i) Any duty of confidentiality owed to the other individual;
  (ii) Any steps taken by the data controller with a view to seeking the consent of the other individual
  (iii) Whether the other individual is capable of giving consent; and
  (iv) 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 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 in 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.

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:

  (i) The supply of such a copy is not possible or would involve disproportionate effort; or
  (ii) The data subject agrees otherwise
  (iii) 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 purpose 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 a 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 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 referred to in its entirety.

Appendix C

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.

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

After considerable research and consultation, the nationally recommended standard of the CCTV User Group has been adopted by Spelthorne Borough Council

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

- 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

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

  i) Police
  ii) Statutory Authorities with powers to prosecute, (e.g Customs and Excise; Trading Standards, etc)
  iii) Solicitors
  iv) Plaintiffs in civil proceedings
  v) Accused persons or defendants in criminal proceedings
  vi) Other agencies , (which should be specified in the Code of Practice) according to purpose and legal status
- 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 the 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 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)

- In circumstances outlined at note (3) below, (requests by palintiffs, 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 to be restricted to the Civil Police but could include, (for examples) 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 (eg to the nearest ½ hour)

Secondary Request To View Data

- 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, (eg Data Protection Act 2003, Human Rights Act 2003)
  ii) Any legislative requirements have been complied with, (eg 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

- 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 a personal knowledge of the circumstances of the crime/s to be prevented and an understanding of the CCTV System Code of Practice

ii) If the material is to be released under the auspices of 'public' well being, health or safety, written agreement to the release of the 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.

- 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

Notes

(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 wellbeing
   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.

4 Individual Subject Access under Data Protection Legislation

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

i) The request is made in writing
ii) A specified fee is paid for each individual search;
iii) The data controller is supplied with sufficient information to satisfy him or 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

- 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

- 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.

- 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

- Verify the accuracy of the request
- Replay the data to the requester only (or responsible person acting on behalf of the person making the request)
- The viewing should take place in a separate room and not in the control room or monitoring area. Only data which is specific to the search request shall be shown.
- It must not be possible to identify any other individual from the information being shown (any such information will be blanked out, either by means of electronic screening or manual editing on the monitor screen).
- If a copy of the material is requested and there is no on-site means of editing out other personal data, then the material shall be sent to aqn editing house for processing prior to being sent to the requester.

Notes

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

7. Media Closure

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;

- 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, eg specific identities/data that must not be revealed.
  iii) It shall require that the 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 Systems Codes 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 to the requirements of the Information Commissioner in this respect detailed in the Code of Practice summarised above

8. Principles

In adopting this national standard for the release of data to third parties, it is intended, as far as reasonably practicable, to safeguard the individuals 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 the Code of Practice for the CCTV scheme;
- Access to recorded material shall only take place in accordance with this standard and the Code of Practice;
- The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

Appendix ‘D’

Restricted Access Notice

Warning

Restricted Access Area

Everyone entering this area, regardless of status, 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 CCTV monitoring room is, and should remain, confidential. You agree not to divulge any information obtained, overheard or seen 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 Spelthorne Borough CCTV System

I …… am retained by Spelthorne Borough Council to perform the duty of CCTV operator. 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 the Code of Practice and understand that all duties which I undertake in connection with the Spelthorne 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 unclear on any aspect of the operation of the system or the content of the Code of Practice, I undertake to seek clarification the issues.

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 Spelthorne Borough Council may be an offence against the Official Secrets Act 1911, Section 2, as amended by the Official Secrets Act 1989.

Signed …… Print name ……..

Witness ……. Position …….

Date ……..

Appendix F

Subject Access Request Form

Appendix F Subject Access Request Form **

‘Spelthorne Council’ 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. Spelthorne 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)

Spelthorne Borough Council Rights

Spelthorne 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 **'Spelthorne 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. Spelthorne 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 Community Safety Manager, Spelthorne Borough Council,
Civic Offices, Knowle Green, Staines Upon Thames, TW18 1XB.
(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. 01784 446322/444226

Spelthorne Borough Council 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 about you.

Tilte (Mr/Mrs/Miss/MS) ……

Other title (Dr/Rev etc) ……..

Surname/family name ……..

First names ……..

Maiden Name/former names ……..

Sex ……..

Height ……..

Date of Birth ……..

Place of birth (Town & County) ……..

Your Current Home Address ……

(to which we will reply) ……

Tel nos ……

If you have lived at the above address for less than 10 years, please give your previous addresses for that period including dates of occupancy.

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 you name and address

Also a recent, full face photograph of yourself

Failure to provide this proof of identity may delay your application

Section 3 Supply of Information

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

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

(b) Only view the information Yes/No

Section 4 Declaration

Declaration (to be signed by the applicant)

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

Signed ……. Date ……

Appendix G

Use of Mobile CCTV System

Introduction

Mobile Closed Circuit Television (CCTV) Systems may be operated within Spelthorne 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 Community Safety recording/reviewing 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.

Objectives of the system

The objectives of the mobile system which can be deployed rapidly are:

- 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 preventative 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 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 a total respect for everyone's right to respect for his or her private and family life and their home. All data will be processed in accordance with the principles of the Data Protection Act 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 a 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. The Act 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 in the 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 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:Part 1 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 a fair trial) and the evidence obtained could be excluded in Court under Section 78, Police and Criminal Evidence Act 1981 (?)

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

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 11 – 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 the 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 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 wil 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 states;

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 purpose of the investigation or operation);

And otherwise than by way of an immediate response to events or circumsatnces 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/her 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 only be authorised by chief officers within UK police forces and HMRC and it 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 are listed in Schedule 1/Part 1, in respect of Directed surveillance are detailed in Article 2/Part 1- Statutory Instrument

2417/2000: The Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) Order 2000.

e.g

For a Local Authority (within the meaning of Section 1 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 – Maintained under Section 2 of the Police Act 1996 (Forces in England & Wales) the prescribed level is Superintendent or Inspector in urgent cases.

The impact for staff in police control rooms and CCTV monitoring rooms 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 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

(i) In the interests of national security
(ii) For the purposes of preventing or detecting crime or of preventing disorder
(iii) In the interests of the economic well-being of the UK
(iv) In the interests of public safety
(v) For the purpose of protecting public health
(vi) For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or
(vii) 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 rationale clearly articulated 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 the above principles.

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:

Inspector 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 ask CCTV to watch the vehicle over a period of time (no longer a response to immediate events) and note who goes to and from the vehicle – *sustained surveillance of individual(s) gaining private information.*

Superintendent Authorisation

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 they wish to have the cameras monitor them instead, so as not to divulge the observation taking place – *response to immediate events.*

Access to all relevant information on this Act, including the Schedules and Statutory Instruments referred to in this guidance can be obtained from the Home Office website

Appendix I

Formulation, Application, and Liability

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 UK 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 and Investigations Act 1996; Codes – Police & Criminal Evidence Act 1984 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. The collective work by all the individuals and organisations involved has greatly assisted in the preparation of this document.