

Rushmoor Borough Council

Code of Practice
for the operation of
Closed Circuit Television



July 2003

Contents

	Section
Introduction and Objectives	1
Principles of Operation	2
Privacy and Data Protection	3
Accountability and Public Information	4
Assessment of the System and the Code of Practice	5
Human Resources	6
Control and Operation of the Cameras	7
Access to, and Security of, Monitoring Room and / or Associated Equipment	8
Management of Recorded Material	9
Video Prints	10
Appendices	
Key Personnel and their Responsibilities	A
Extracts from the Data Protection Act, 1998 and other information	B
Releasing Data to Third Parties	C
Declaration of Confidentiality	D

Section 1 Introduction and Objectives

Introduction

An integrated Closed Circuit Television (CCTV) System has been introduced to Aldershot, Farnborough and North Camp and will be known as the Rushmoor CCTV System (the System). The System has evolved from individual town centre schemes operated in partnership with Rushmoor Borough Council but controlled by retail security staff at the relevant shopping centres.

The Rushmoor CCTV System comprises of a number of cameras installed at various strategic locations throughout the Borough including streets, parks, public places, car parks and Council premises.

All cameras are monitored and controlled by a central control room located within the main council offices in Farnborough. Secondary monitoring without direct control is possible at other locations. At the present time monitoring is only available to retail security staff in Aldershot (The Galleries) and Farnborough (Princesmead and Kingsmead) shopping centres.

Radio communication links have been established with the police, Aldershot and Farnborough Town Link Radio users and other council services.

The Rushmoor CCTV System is supported by the Rushmoor Community Safety Partnership and managed by Rushmoor Borough Council. Genesis Security Ltd on the Council's behalf undertakes monitoring and the day-to-day operation of the System.

The System is managed by the Community Safety Manager who is also designated the CCTV Manager for the purposes of this Code of Practice.

The primary legislation governing the operation of the System is the Data Protection Act 1998, the Human Rights Act 1998 and the Regulation of Investigatory Powers Act 2000.

Purpose of the System

The purposes of the Rushmoor CCTV are

- To help prevent, detect and reduce crime and disorder
- To help reduce the fear of crime and increase feelings of safety
- To provide evidence to assist in criminal and civil cases
- To assist the police to deploy their resources effectively
- To assist Rushmoor Borough Council in discharging its duties
- To monitor the safety of the public, Rushmoor Borough Council staff and employees of the Council's authorised contractors
- To protect Council properties
- To monitor traffic flow and assist in traffic management matters
- To assist in civil emergencies

Rushmoor Borough Council's statement in respect of The Human Rights Act 1998

The 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 1998, and consider that the use of CCTV in Rushmoor is a necessary, proportionate and suitable tool to help reduce crime, reduce the fear of crime and improve public safety. Continuing consultation evidences this assessment. 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. Rushmoor Borough Council also considers it a key initiative towards its duty under the Crime and Disorder Act 1998.

It is recognised that operation of the System may be considered to infringe on the privacy of individuals. Rushmoor Borough Council recognises that it is its responsibility to ensure that the System should always comply with all relevant legislation, to ensure its legality and legitimacy. The System will only be used as a proportionate response to identified problems and be used only in so far as it is necessary in a democratic society, in the interests of national security, public safety and preventing and detecting crime and disorder.

The Code and the observance of the operational procedures contained in the Procedure 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 fair trial.

The 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.

Procedure Manual

The Code is supplemented by Rushmoor Borough Council's 'Procedure Manual' which offers instructions on all aspects of the day-to-day operation of its Control Room and tape management. The Procedure Manual will be retained in the Control Room.

Section 2 Principles of Operation

General Principles

The System will be operated

- in accordance with all the requirements and the principles of the Human Rights Act 1998.
- to recognise the need for formal authorisation of any covert 'directed' surveillance as required by the Regulation of Investigatory Powers Act 2000 and the requesting organisation's policy.
- in accordance with the Data Protection Act 1998 at all times
- fairly, within the law, and only for the purposes for which it was established and are identified within the Code, or which are subsequently agreed in accordance with the Code.
- with due regard to the principle that everyone has the right to respect for his or her private and family life and their home.
- To ensure that public interest will be recognised by ensuring the security and integrity of operational procedures.

Throughout the Code it is intended, as far as reasonably possible, to balance the objectives of the System with the need to safeguard the rights of individuals. Every effort has been made throughout the Code to indicate that a formal structure has been put in place, including a complaints procedure, by which it can be identified that the System is not only accountable, but is seen to be accountable.

Participation in the System by any organisation, individual or authority assumes an agreement by all such participants to comply fully with the Code and to be accountable under it.

UNLESS SPECIFIED IN THE CODE NO UNAUTHORISED USE OF THE SYSTEM FOR ANY OTHER PURPOSE SHALL BE PERMITTED.

Copyright

Copyright and ownership of all material recorded by virtue of the System will remain with Rushmoor Borough Council.

Cameras and Area Coverage

The Rushmoor CCTV System comprises of a number of cameras installed at various strategic locations throughout the Borough including streets, parks, public places, car parks and Council premises.

Details of the locations of all cameras are available in the CCTV Control Room. Appropriate signs identify the presence of cameras.

Monitoring and Recording Facilities

A Control Room is located at the Rushmoor Borough Council Offices, Farnborough Road, Farnborough. This monitoring facility will be staffed 24 hours a day throughout the year, including Bank Holidays. The CCTV equipment in the Control Room has the capability of recording from all cameras simultaneously throughout every 24-hour period.

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 are able to

control and view images from selected cameras. All viewing and recording equipment shall only be operated by trained and authorised users.

Human Resources

The Control Room control room shall be staffed by properly trained employees. All operators will be appropriately supervised and given instruction to make sure that the System is operated in accordance with the law and with proper respect for people's rights.

Processing and Handling of Recorded Material

All recorded material, whether recorded digitally, in analogue format or as a hard copy video print, will be processed and handled strictly in accordance with this Code and the Procedure Manual.

Operators Instructions

Technical instructions on the use of equipment housed within the Control Room are contained in separate manuals provided by the equipment suppliers.

Changes to the Code or the Procedure Manual

Any major changes to either this Code or the Procedure Manual, (i.e. such as will have a significant impact upon the Code or upon the operation of the System) will take place only after consultation with the Head of Information Services and the Solicitor to the Council.

A minor change, (i.e. such as may be required for clarification and will not have such a significant impact) may be made by the CCTV Manager.

Section 3 Privacy and Data Protection

Public Concern

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 personal data*' 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 respect for everyone's right to his or her private and family life and their home.

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

Data Protection Legislation

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

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

- All personal data will be processed fairly and lawfully.
- Personal data will be held only for the purposes specified.
- Personal data will be used only for the purposes, and disclosed only to the people, shown within the Codes.
- 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, or loss and destruction of, information.

Request for information (subject access)

Any request from an individual for the disclosure of personal data which he / she believes is recorded by virtue of the System will be directed to the Data Protection Officer

The principles of Sections 7 and 8 of the Data Protection Act 1998 (Rights of Data Subjects and Others) shall be followed in respect of every request. 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 expect from being in that location at that time) in accordance with the requirements of the legislation.

Any person making a request must be able to satisfactorily prove their identity and provide sufficient information to enable the data to be located.

Exemptions From the Provision of Information

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

Personal data processed for any of the following purposes -

- the prevention or detection of crime
- the apprehension or prosecution of offenders

are exempt from the subject access provisions in any case 'to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection'.

Section 4 Accountability and Public Information

The Public

For reasons of security and confidentiality, access to the CCTV monitoring facilities is restricted in accordance with the Code. However, in the interest of openness and accountability, anyone wishing to visit such facilities may be permitted to do so, subject to the approval of, and after making prior arrangements with (a) the CCTV Manager or (b) the Rushmoor CCTV Control Room Supervisor.

A member of the public wishing to register a complaint with regard to any aspect of the System may do so by contacting the CCTV Manager. Any performance issue or complaint identified involving an operator will be dealt with in liaison with the management of Genesis Security Ltd. The System Manager will ensure that every complaint is dealt with expeditiously. The CCTV Manager has the responsibility to advise the complainant of the enquiry procedure to be undertaken.

Code of Practice

The Code shall be made available to view on the Council's website and at Rushmoor Borough Council Offices Farnborough Road, Farnborough between the hours of 9.00am - 5.00pm Monday to Thursday inclusive and 9.00am – 4.30pm on Friday.

Signs

Signs will be placed in the locality of the cameras. The signs will indicate:

- The presence of CCTV monitoring;
- The 'ownership' of the system;
- A contact telephone number for further information.

Section 5 Assessment of the System and Code of Practice

The CCTV Manager in liaison with Genesis Security Ltd will accept day to day responsibility for the monitoring, operation and evaluation of the System and the implementation of the Code. The System Manager shall also be responsible for maintaining management information concerning incidents dealt with by the Control Room for use in evaluation.

Section 6 Human Resources

Staffing of the Control Room

The Control Room will be staffed in accordance with the Procedure 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. Operators will be fully conversant with the contents of the Code of Practice and Procedure Manual, 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.

Arrangements may be made for police officers to be present in the Control Room as operators at certain times, or indeed at all times, subject to locally agreed protocols. Any such person must also be conversant with the Code and associated Procedure Manual.

Discipline

Every individual with any responsibility under the Procedure Manual or the terms of the Code and who has any involvement with the System to which they refer, will be subject to his/her employer's disciplinary policy or procedures. Any breach of the Code or of any aspect of confidentiality will be dealt with in accordance with those discipline rules. A breach of the Code may result in criminal proceedings.

Declaration of Confidentiality

Every individual, other than a police officer who is already bound by a formal confidentiality provision, with any responsibility under the terms of the Code and who has any involvement with the System to which it refers, will be required to sign a declaration of confidentiality. (See Appendix D, see also Section 8 concerning access to the monitoring room by others).

Section 7 Control and Operation of Cameras

Guiding Principles

Any person operating the cameras will act with utmost probity at all times. Every use of the cameras will accord with the purposes and key objectives of the System and shall be in compliance with the Code and all statutory requirements.

Cameras will not be used to look into private residential property unless specifically authorised by the Regulation of Investigatory Powers Act 2000.

Camera operators will be mindful of exercising prejudices which may lead to complaints that the System is being used for purposes other than those for which it is intended. The operators may be required to justify their monitoring, or recording of, any particular individual, group of individuals or property at any time. From time to time the operation of the System will be assessed by the CCTV Manager.

Camera Control

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

Operation of the System by the Police

The Police may make a request to assume direction of the System to which this Code of Practice applies. The Police, where appropriate, will supply evidence of authorisation under the Regulation of Investigatory Powers Act 2000.

Section 8 Access to and Security of Control Room and Associated Equipment

Authorised Access

Only trained and authorised personnel will operate the CCTV equipment in the Control Room.

Public access

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 CCTV Manager or CCTV Control Room Supervisor. Any such visits will be conducted and recorded in accordance with the Procedure Manual.

Declaration of Confidentiality

On entering the Control Room visitors will be shown a notice reminding them of their obligation of confidentiality. Operators will ensure that all visitors sign the visitors book in accordance with the Procedure Manual..

Security

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

Section 9 Management of Recorded Material

Guiding Principles

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

Every video recording used in conjunction with the System has the potential of containing material that has to be admitted in evidence at some point during its life span.

Members of the public 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.

It is therefore of the utmost importance that every means (e.g. video tape) of video recording is treated strictly in accordance with the Code and the Procedure Manual from the moment it is delivered to the monitoring room until its final destruction.

Access to and the use of recorded material will be strictly for the purposes notified to the Information Commissioner.

Copyright and ownership of all material recorded by virtue of the System will remain with the data controller. In order to uphold the integrity of the System and retain control of all recorded data it is important that operators within secondary monitoring facilities do not under any circumstances record images

received from the Rushmoor CCTV System. This will include recording images on to videotape and producing video prints.

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

National standard for the release of data to a third party

Every request for the release of personal data generated by the System will be determined by the CCTV Manager in consultation with the Solicitor to the Council. The CCTV Manager will ensure the principles contained within Appendix C of the Code are followed at all times.

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

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

Members of the police service or other law enforcement 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 Procedure Manual.

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 Procedure Manual.

Video Tapes – Retention

Recorded tapes will be retained for a period of one calendar month. Before reuse or destruction, each tape will be magnetically erased.

Video tapes will be used in accordance with the Procedure Manual. Only video tapes which are part of the System will be allowed in to the Control Room and used in its equipment.

Recording Policy

Subject to the equipment functioning correctly, images from every camera will be recorded throughout every 24 hour period in 12 hour time lapse mode, through digital multiplexers onto S-VHS or VHS video tapes or computer disk. Images from selected cameras will be recorded in real time at the discretion of the CCTV operators or as requested by the police.

Evidential Tapes

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

Section 10 Video Prints

Guiding Principles

A video print is a copy of an image or images. 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 Procedure Manual and the Data Protection Act 1998.

Video prints contain data and will therefore only be released under the terms of Appendix C. If prints are released to the media in an effort to identify alleged offenders or potential witnesses full details will be recorded in accordance with the Procedure Manual. A record will be maintained of all video print productions.

Appendix A Key Personnel and Responsibilities

The Data Controller

Rushmoor Borough Council,

Council Offices, Farnborough Road, Farnborough, GU14 7JU

Tel: 01252 398398

The Data Controller is responsible for determining the Code and adherence to it, that the Procedure Manual is in place and operating and the appointment of a CCTV Manager. Under the provisions of the Data Protection Act 1998, the Council's Head of Information Services is designated.

CCTV Manager

The Rushmoor CCTV Manager is the Rushmoor Borough Council Community Safety Manager located at the above address. (Tel: 01252 398175)

The CCTV Manager is the point of reference on behalf of the Council and his role will include:

- Ensuring the provision and maintenance of all equipment forming part of the Rushmoor CCTV System in accordance with contractual arrangements.
- Maintaining close liaison with Genesis Security Ltd
- Ensuring the interests of the Council is upheld in accordance with the terms of this Code of Practice.
- Implementing any alterations and additions to the System, this Code or the Procedure Manual.

Data Processors

The Data Processor is Genesis Security Ltd

The responsibilities of data processors include:

- The day-to-day operation and administration of the Rushmoor CCTV Control Room.
- The provision and supervision of trained operators.
- Maintaining a close liaison with the CCTV Manager and representing him or her as agreed.

The Data Processor will be responsible for ensuring compliance with the Code of Practice and appropriate Procedure Manuals.

Appendix B Extracts From Data Protection Act 1998

Section 7

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

- (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, and 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,
- (b) 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;
 - iii) 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 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 any duty of confidentiality owed to the other individual,
 - (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

- (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.

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:

the supply of such a copy is not possible or would involve disproportionate effort, or

the data subject agrees otherwise;

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.

Appendix C Releasing Data to Third Parties

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, but must also be used in a manner which stands up to scrutiny and is accountable to the very people they are aiming to protect.

Rushmoor Borough Council and all other partner organisations involved in the operation of this System 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.

The nationally recommended standard of The CCTV User Group has been adopted by the System owner.

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 notified to the Information Commissioners.
- 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.

General Policy

All requests for the release of data shall be processed in accordance with the Procedure Manual. The processing of all such requests shall be the responsibility of the CCTV Manager although in day-to-day practice this may be devolved to the CCTV Control Room Supervisor.

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

- (i) Police (note 1)
- (ii) Statutory authorities with powers to prosecute, (e.g. Customs and Excise; Trading Standards, etc.)
- (iii) Solicitors (note 2)
- (iv) Plaintiffs in civil proceedings (note 3)
- (v) Accused persons or defendants in criminal proceedings (note 3)
- (vi) Other agencies, (which should be specified in the Code) according to purpose and legal status (note 4).

Upon receipt from a third party of a request for the release of data, the CCTV Manager shall in consultation with the Solicitor to the Council if necessary:

- (i) Take the steps required to ensure that the request is relevant, valid and for a proper purpose.
- (ii) Not unduly obstruct a third party investigation to verify the existence of relevant data.
- (iii) 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.

In circumstances outlined at note (3) below, (requests by plaintiffs, accused persons or defendants) the CCTV Manager, or nominated representative, shall:

- (i) Be satisfied that there is no connection with any existing data held by the police in connection with the same investigation.
- (ii) Treat all such enquiries with strict confidentiality.

Notes

- 1) *The release of data to the police is not restricted to the civil police but could include British Transport Police, Ministry of Defence Police, Military Police, etc.*

- 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 the 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 CCTV Manager, in consultation with the Solicitor to the Council, 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*

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 CCTV Manager in consultation with the Solicitor to the Council shall ensure that:

- (i) The request does not contravene, and that compliance with the request would not breach, current legislation, (e.g. Data Protection Act 1998, Human Rights Act 1998, section 163 Criminal Justice and Public Order Act 1994);

- (ii) 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
- (iii) The request would pass a test of 'disclosure in the public interest' (note 1)

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 allowing access to the material:

- (i) In respect of material to be released within the category 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 (note 2)
- (ii) If the material is to be released in the interests of the health or safety of the public as a whole, written agreement to the release of material should be obtained from the Chief Executive, Director or Head of Service. 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.

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 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,

Individual Subject Access Under Data Protection Legislation

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 £10 fee is paid for each individual search;
- (iii) The CCTV Manager is supplied with sufficient information to satisfy him or her self as to the identity of the person making the request;
- (iv) The person making the request provides sufficient and accurate information about the time, date and place to enable the data controller to locate the information which that person seeks,
- (v) The person making the request is only shown information relevant to that particular search and which contains personal data of her or him self only, unless all other individuals who may be identified from the same information have consented to the disclosure;

In the event of the CCTV Manager 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 CCTV Manager 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 Act, the CCTV Manager 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)

Process of Disclosure:

In the event of the CCTV Manager complying with a request to supply data he/she shall;

- (i) Verify the accuracy of the request.
- (ii) Replay the data to the requestee only, (or a person acting on behalf of and appointed by the person making the request).
- (iii) 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.
- (iv) 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).
- (v) If a copy of the material is requested and there is no on-site means of editing out other personal data, then the material shall be sent to an editing house for processing prior to being sent to the requestee.

Media disclosure

Set procedures for the release of data to a third party should be followed.

- (i) 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:
- (ii) 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.
- (iii) 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.
- (iv) It shall require that proof of any editing must be passed back to the data processor 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).
- (v) The release form shall be considered a contract and signed by both parties⁽¹⁾.

Note

In the 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 accidental broadcast in the future..

Rushmoor CCTV System

Declaration of Confidentiality



This confidentiality agreement acknowledges that my duties allow me access to the Rushmoor CCTV Control Room or data processed by the System.

I agree that I have read the Code of Practice in respect of the operation and management of that CCTV System. and hereby declare that:

- (a) I am fully conversant with the content of that Code of Practice and understand that all duties which I undertake in connection with the Rushmoor 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.

- (b) I understand that I must 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 Rushmoor 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.

Signed:Print Name:.....

Position

Date: