CCTV Code of Practice

Version 1

August 2013

1. Introduction

This Code of Practice shall apply to the closed circuit television surveillance scheme known as the Rossendale Borough Council CCTV scheme. The scheme comprises overt surveillance cameras located in specific external locations within the Rossendale Borough Council area, with recording facilities either in each camera or at a central location, depending on the site of the camera.

This Code of Practice is issued in accordance with the following guidance:

- Surveillance Camera Code of Practice (Home Office: June 2013)

- CCTV Code of Practice (Information Commissioners Office: Revised Edition 2008)

- Subject Access Code of Practice (Information Commissioner's Office: August 2013)

- CCTV Operational Requirements Manual (Home Office: 2009).

This code of practice does not cover any Rossendale Borough Council CCTV cameras located internally or externally for the sole purpose of protection and surveillance of council staff and / or buildings. It also does not extend to surveillance systems operated by private organisations or individuals.

This code of practice will be implemented in line with the Council's Equality Policy and associated duties.

2. Ownership

The scheme is owned by Rossendale Borough Council who is responsible for the management, administration and security of the system. As such the Council will ensure the protection of individuals and the public by complying with the Code of Practice.

Rossendale Borough Council is registered with the Information Commissioner's Office as the data controller for the CCTV system. This is reviewed on an annual basis.

3. Closed Circuit Television Mission Statement

To promote public confidence by developing a safe and secure environment for the benefit of those living in, employed in, or visiting the areas covered by the CCTV schemes.

4. Code of Practice Mission Statement

To inspire public confidence by ensuring that all public area Closed Circuit Television (CCTV) systems are operated in a manner that will secure their consistent effectiveness and preserve the civil liberty of law abiding citizens at all times.

5. Definitions

- The CCTV 'data centre' shall mean the secure area of a building where CCTV data is retrieved and processed.
- 'CCTV scheme' shall mean the totality of the arrangements for closed circuit television in the locality and is not limited to the technological system, staff and operational procedures.
- The 'retrieval system' means the capability, in any medium, of effectively capturing data that can be retrieved, viewed or processed.
- 'CCTV system' means the surveillance items comprising cameras and associated equipment.
- 'Data' shall mean all information, including that about a person in the form of pictures, and any other associated linked or processed information.
- 'Personal Data' means data which relates to a living individual who can be identified:
  - from that data or
  - from that data and other information which is in the possession of or is likely to come into the possession of, the data controller.
- 'Sensitive personal data' is personal data which is deemed to be sensitive. The most significant of these, for the purposes of this code are information about:-
  - The commission or alleged commission of any offences
  - Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.
- An 'incident' is an activity that raises cause for concern that the safety or security of an individual or property including vehicles may be compromised or that an offence has been committed, or that an occurrence has taken place warranting specific action by an operator.
- The 'Owner' is Rossendale Borough Council, the organisation with overall responsibility for the formulation and implementation of policies, purposes and control of the scheme.
- The 'Manager' has the responsibility for the implementation of the policies, purposes and methods of control of a CCTV scheme, as defined by the owner of the scheme. The manager of the scheme is a designated employee of Rossendale Borough Council.
- 'Data controller' means a body or 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, or are about to be processed. The Data Controller for the CCTV scheme is Rossendale Borough Council. Once an image or footage has been disclosed to another body, such as the police, they become the data controller for their copy of that image or footage. It is

their responsibility to comply with relevant legislation and codes of practice in relation to any further disclosures.

- 'Operators' are employees of Rossendale Borough Council or contractor employed by the Council, and are specifically designated to carry out the physical operation of controlling the CCTV system and the data generated.
- 'Recording material' means any medium that has the capacity to store data and from which data can later be recalled irrespective of time.
- A 'hard copy print' is a paper copy of a live image or images, which already exist on recorded material.
- The 'Surveillance Camera Commissioner' is a statutory appointment made by the Home Secretary whose statutory functions are: encouraging compliance with the Home Office Code of Practice; reviewing the operation of the code; providing advice about the Code.

6. System description

The CCTV system referred to in this document is owned by Rossendale Borough Council and its implementation and/or expansion is supported by the following bodies (the partners)

- Lancashire Police
- Community Safety Partnership

The owner, manager, supervisor, operator and all partners will work in accordance with this Code. The partners will have no involvement in the operating of the system.

The system consists of closed circuit television cameras in the Bacup, Stacksteads, Haslingden and Rawtenstall areas, primarily focused in town centres.

The recording material of the cameras varies according to the location of the camera, and includes hard drives, secure wireless access and ethernet links with the Rossendale Borough Council data centre.

The cameras are able to pan, tilt, zoom or remain fixed and are contained in vandal resistant units.

Images from all cameras are recorded simultaneously throughout a 24 hour period 365 days each year. Footage is recorded and stored for up to 31 days then automatically recorded over on a rolling basis.

The images recorded are full colour but when light levels drop the units switch to monochrome to provide a better low light capability. There is no audio recording facility in the cameras.

Signage is installed in town centre locations informing the public that surveillance cameras are in operation, who is operating the system and the purpose.

The physical and intellectual rights in relation to any and all material recorded from the CCTV cameras shall at all times remain in the ownership of Rossendale Borough Council.

7. Changes to the Code of Practice

Any major changes to this Code of Practice will take place only after consultation with stakeholders and the Council's Scheme of Delegation procedure has been followed.

Major changes to this code are defined as changes that affect its fundamental principles and shall be deemed to include:

- Additions and omissions of cameras to the system
- Matters which have privacy implications
- Additions to permitted uses criteria e.g. purposes of the scheme
- Changes in the right of access to personal data, except statutory requirements
- Significant legal implications.

Minor changes to this Code of Practice are defined as operational and procedural matters which do not affect the fundamental principles and purposes; these include:

- Change of contractors involved in the supply or operation of the system (subject to procurement rules)
- Additional clarifications, explanations and corrections to the existing code
- Additions to the code of practice in order to conform to the requirements of any statutory Acts and changes in criminal legislation

A minor change may be agreed between the Manager of the system and the Portfolio Holder.

The Code of Practice will be subject to annual review which will include compliance with the relevant legislation and Standards.

8. Purpose of and Compliance with the Code of Practice

This Code of Practice is to detail the management, administration and operation of the CCTV system in the Rossendale Borough Council area.

The Code of Practice has a dual purpose, in that it will assist owners, management and operators to understand their legal and moral obligations whilst reassuring the public about the safeguards contained within it.

The owners, operators and users of the CCTV system and associated safety and security equipment shall be required to give a formal undertaking that they will

comply with this Code of Practice and act in good faith with regard to the basic principles contained within it.

The owners, operators, users and any visitors to the data centre or other council facility for the purpose of viewing CCTV footage will be required to sign a formal confidentiality declaration that they will treat any viewed and/or written material as being strictly confidential and that they undertake not to divulge it to any other person. A copy of this declaration is attached at Appendix A.

9. Objectives of the scheme

The following objectives have been established for the Rossendale Borough Council CCTV system:

(a) Reducing the fear of crime

(b) Deterring and preventing crime

(c) Assisting in the maintenance of public order and tackling offences involving vandalism and nuisance

(d) Providing high quality evidence which may assist in the detection of crime and the apprehension and prosecution of offenders

(e) Protecting property

(f) Providing assistance with civil claims

(g) Providing assistance with issues relating to public safety and health

10. Rights of Privacy

Rossendale Borough Council and partners support the individual's right to privacy and will insist that all agencies involved in the provision and use of public surveillance CCTV systems connected to the control, monitoring and recording facility accept this fundamental principle as being paramount.

11. Principles of management of the scheme

The cameras have been sited to capture images that are relevant to the specified purposes for which the scheme has been established.

Cameras are sited to ensure that they can produce images of the right quality, taking into account technical and environmental issues

The scheme will be operated fairly, within the applicable law and only for the purposes for which it is established or which are subsequently agreed in accordance with the Code of Practice.

Operators are aware of the purpose(s) for which the scheme has been established and that the CCTV equipment is only used to achieve the identified purposes.

The scheme will be operated with due regard for the privacy of the individual.

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

The system will only be operated by trained and authorised personnel.

Prior to the installation of additional cameras an 'Impact Assessment' to determine whether CCTV is justified and how it will be operated will be undertaken in compliance with the Information Commissioners CCTV Code of Practice

To accomplish the above an 'Operational Requirement' checklist will be completed at the time of the 'Impact Assessment' for each proposed camera to dictate the quality of images required. This is a recommendation of the information Commissioner and will be carried out in accordance with the CCTV Operational Requirements Manual (Home Office: 2009).

Before cameras are placed in residential areas the residents in that area will be consulted concerning the proposed system and the results of the consultation will be taken into account.

12. Supplementary Documentation

The procedure which will be followed in retrieving and processing CCTV footage is contained within Appendix B to this document.

13. Point of contact

Should members of the public wish to make contact with the owners of the scheme they may write to:

CCTV Manager, Rossendale Borough Council
The Business Centre, Futures Park,
Bacup, OL13 OBB

14. Release of information to the public

Information will be released to third parties, itemised in Section 25, who can show legitimate reasons for access. They will be required to request any information with reasons in writing and identify themselves. Information will only be released if the data captures identifiable individuals or information relating to individuals and the reasons are deemed acceptable; the request and release of information complies with current legislation; and on condition that the information is not used for any other purpose than that specified.

Individuals may request to view information concerning themselves held on record in accordance with the Data Protection Act 1998. The procedure is outlined in Section 25.9 of this Code of Practice.

15. Release of information to statutory prosecuting bodies

The policy is to assist statutory prosecuting bodies such as the Police, and statutory authorities with powers to prosecute and facilitate the legitimate use of the information derived from the scheme. Statutory bodies may have access to information permitted for disclosure on application to the owner of the scheme or the manager, provided the reasons and statement of purpose, accord with the objectives of the scheme and conditions outlined in section 25. The information will be treated as evidential exhibits.

16. Policy review

There will be a policy review every 3 years covering the following aspects:

a) Whether the purpose and objectives statements remain valid

b) Change in extent of the scheme

c) Contracts with suppliers

d) A review of the data protection or legal requirements

e) Maintenance schedule and performance test of the system

f) Scheme evaluation findings

g) Complaints procedure and evaluation

17. Relevant Legislation

17.1 Data Protection

The scheme is registered with the Information Commissioner. The scheme will be managed in accordance with the principles of the Data Protection Act 1998. The Act encompasses eight Data Protection Principles a summary of which is attached at Appendix D.

17.2. Human Rights Act 1998

The scheme and those connected with it acknowledges the provisions within the Human Rights Act 1998 and its impact on issues relating to the use of CCTV. The scheme is considered necessary for the purposes already outlined and to fulfil the requirements of the Crime and Disorder Act 1998. The system will be used proportionally, legally and remain accountable.

17.3. Criminal Procedures and Investigations Act 1996

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

17.4. Freedom of Information Act 2000 (FOIA)

If a request for images is received via a FOIA application and the person requesting is the subject, these will be exempt from the FOIA and will be dealt with under The Data Protection Principles as a subject access request.

Any other requests not involving identification of individuals can be disclosed but only if it does not breach The Data Protection Principles.

17.5. Regulation of Investigatory Powers Act 2000

Introduction

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

Background

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

Neither do the provisions of the Act cover the normal, everyday use of overt CCTV surveillance systems. Members of the public are aware that such systems are in use, for their own protection, and to prevent crime. However, it had not been envisaged how much the Act would impact on specific, targeted use of public/private CCTV systems by ‘relevant Public Authorities’ covered in Schedule 1: 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 1998 (Right to fair trial) and the evidence obtained could be excluded in court under Section 78 Police & Criminal Evidence Act 1984.

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". Both types of surveillance if part of a pre-planned operation will require authorisation from specified persons named in the Act. In addition, the reasons for such surveillance must be clearly indicated and fall within the criteria outlined by this legislation. A procedure is in place for regular reviews to be undertaken into authorisation.

Any Rossendale Borough Council scheme will observe the criteria laid out in the legislative requirements.

18 Support of Principles

Rossendale Borough Council and the Partners support the principle that the community at large should be satisfied that the Public Surveillance CCTV systems are being used, managed and controlled in a responsible and accountable manner and that in order to meet this objective there will be independent assessment and scrutiny. It is the responsibility of all parties to maintain a continuous review of its' integrity, security, procedural efficiency, methods of operation and retention and release of data.

19 Hierarchy of Responsibilities

19.1 The Owner

The owner of the system has overall responsibility for its operation. The owner is responsible for dealing with complaints, and the role of the owner includes all statutory responsibilities including the role of "data controller" as prescribed by the Data Protection Act 1998 Section 1 Subsection 1(1).

The owner of the system is Rossendale Borough Council.

19.2 The Manager

The manager or designated member of staff should undertake regular reviews of procedures to ensure that the provisions of this Code are being complied with. These should be reported back to the owner of the scheme.

The manager is the person who has direct control of the scheme and as such he/she will have authority for the following:

- Staff management
- Observance of the policy and procedural practices

- Release of data to third parties who have a legal right to copies
- Control and security clearance of visitors
- Security and storage of data
- Security clearance of persons who request to view data
- Release of new and destruction of old data and recorded material
- Liaison with police and other agencies
- Maintenance of the quality of recording and monitoring equipment

The manager may delegate some or all of these authorities to the supervisor as appropriate to ensure the effective and efficient operation of the scheme.

The manager should retain responsibility for the implementation of procedures to ensure that the system operates according to the purposes for which it was installed and in accordance with the objectives identified for the system.

The manager of the system is the Director of Customers & Communities.

19.3 The Supervisor

The supervisor has a responsibility to ensure that at all times the system is operated in accordance with the policy and all procedural instructions relating to the system, and for bringing to the immediate attention of the manager any matter affecting the operation of the system, including any breach or suspected breach of the policy, procedural instructions, security of data or confidentiality.

The supervisor or designated person should ensure that at all times operators carry out their duties in an efficient and responsible manner, in accordance with the objectives of the scheme. This will include regular checks and audit trails to ensure that the documentation systems in place are working effectively. These systems include:

The CCTV request log
The operators log
Witness statements
Faults and maintenance records
The security of data
Audit logs
Authorisation of visitors – to be checked & counter signed by the Supervisor

The supervisor shall also ensure that on a day-to-day basis all equipment is working correctly and that the operators of the scheme comply with the Code of Practice Procedure. Dealing with breaches of the codes and disciplinary measures shall lie with the manager.

The supervisor will ensure operators comply with Health and Safety Regulations.

The supervisor is a Locality Manager in the Communities Team.

19.4 The Operators

The operators will be responsible for complying with the code of practice and procedure. They have a responsibility to respect the privacy of the individual, understand and comply with the objectives of the scheme. They are required to be proficient in the control and the use of the CCTV camera equipment, recording and playback facilities, media procedures and maintenance of all logs. The information recorded must be accurate, adequate and relevant to the purpose of the scheme. They should bring to the attention of the supervisor immediately any equipment defect that may occur.

The operators of the system will be a Technical Officer in the Communities Team and a designated ICT Officer.

19.5 Accountability

The manager shall be accountable to the owner of the scheme and will provide periodic progress reports on the scheme.

The supervisor will be accountable to the manager of the scheme and will resolve technical and operational matters.

Failure of the operators to comply with the procedure and code of practice will be dealt with by the manager. Person(s) misusing the system will be subject to disciplinary or legal proceedings in accordance with the Council's policies.

20. Audit

Independent audits carried out by Lancashire County Council will periodically check the operation of the scheme and the compliance with the code of practice. Internal audits will be carried out by the Manager of the scheme. They will consider the following:

- The level of attainment of objectives and procedures
- Random audits of the data log and release of information
- The review policy
- Standard costs for the release of viewing of material
- The complaints procedure
- Compliance with procedures

21. Complaints

A member of the public wishing to make a complaint about the system may do so through Rossendale Borough Council's complaint procedure. Copies of the complaints procedure are available from www.rossendale.gov.uk or from the One Stop Shop, The Business Centre, Futures Park, Bacup.

In summary complaints can be made in writing to:

Complaints
Rossendale Borough Council
The Business Centre, Futures Park,
Bacup, OL13 OBB

Alternatively by submitting an online form at http://tinyurl.com/bt3jrtv or by downloading and returning a complaint form available at: http://tinyurl.com/cllxbz2

When a complaint is made a written acknowledgement will be sent on receipt.

An investigation will follow and a written answer will be sent to the complainant within a further ten working days stating that:-

- The investigation will take longer than 10 days and an estimated further response time.
- The investigation is complete giving details of any proposed action. Should a complainant not be satisfied there is an appeals procedure and this is detailed in the full complaints procedure.
- Once a complaint has been concluded the complainant should be advised about regulatory bodies who may have jurisdiction in that complaint such as the Information Commissioner or the Investigatory Powers Tribunal.

A record of the number of complaints or enquiries received will be maintained together with an outline of the action taken and these will be reported on a quarterly basis.

Information about the nature of complaints received about the Council's CCTV system will be shared with the Surveillance Camera Commissioner on request to assist with the review of relevant government codes of practice.

22. Personnel

22.1 Security screening

All personnel employed to control/operate or supervise the scheme will undergo an enhanced security check.

22.2 Training

All operators will be fully trained in use of the equipment to retrieve footage.

Each operator will be issued with a copy of this Code and given training to ensure compliance at all times.

22.3 Contractors

Only appropriately trained and vetted contractors will have access to the system. Wherever possible contractors should not have sight of any recorded data and will be required to sign the Declaration of Confidentiality.

23. Access to the Data Centre and Cameras

Security of the Data Centre shall be maintained at all times.

Only the Supervisor, Operators and designated members of the ICT team will have access to the Data Centre, which has secure access, and only the ICT Manager and Operators will have access to the equipment to access the CCTV cameras.

Should a Police Officer require to view images of relevant CCTV cameras at the Data Centre as part of an investigation of a criminal incident, this will take place by prior appointment and will be supervised by the ICT team or CCTV supervisor.

All visitors to the Data Centre, including Police Officers, will be required to sign the Declaration of Confidentiality.

Only trained operators will access data directly from cameras on site.

Should a Police Officer require to view footage from any of the cameras (other than on recorded material or at the data centre) as part of the investigation of a criminal incident, this will also be by prior appointment only and will be in a private room and supervised by the Supervisor of the scheme.

Any equipment used to access data will have secure access restricted to the Manager, Supervisor and Operator.

24. Privacy

Cameras will not be used to infringe the individual's rights of privacy. The cameras generally are sited where they will not be capable of viewing any residential properties. If it is found there is a possibility that cameras would intrude in private areas, privacy zones would be programmed into the cameras where possible and CCTV operators trained to recognise privacy issues.

25. Disclosure Policy

25.1 The Principles of Disclosure

In accordance with the Information Commissioner's Office CCTV Codes of Practice, The Home Office Surveillance Camera Code of Practice, The FOIA and the Data Protection Act 1998, the following principles must be adhered to:

- All employees will be aware of the restrictions set out in this Code of Practice in relation to access to, and disclosure of, recorded images

- Images not required for the purposes of the scheme will not be retained longer than necessary. However, on occasions it may be necessary to retain images for longer period, where a law enforcement body is investigating a

crime to give them the opportunity to view the images as part of an active investigation

- Images will only be disclosed to third parties who intend processing the data for purposes which are deemed compatible with the objectives of the CCTV scheme, and taking account of relevant legislation and guidance

- Monitors displaying images from areas in which individuals would have an expectation of privacy will not be viewed by anyone other than authorised employees of the user of the equipment.

- Recorded material will only be used for the purposes defined in the objectives and policy

- Access to recorded material will be in accordance with policy and procedures

- Information will not be disclosed for commercial purposes or entertainment purposes

- All access to the medium on which the images are recorded will be documented

- Access to recorded images will be restricted to those staff who need to have access in order to achieve the purpose(s) of using the equipment

- Viewing of the recorded images should take place in a restricted area

25.2 Conditions of disclosure

Before data is viewed by a third party the manager should be satisfied that data is:

a) The subject of a complaint or dispute that is unanswered

b) The original data and the audit trail is maintained throughout

c) Not part of a current criminal investigation by the Police, or likely to be so

d) Not part of civil proceedings or likely to be so

e) Not removed or copied without proper authority

f) The image obtained is aimed at identifying individuals or information relating to an individual.

25.3 Access to recorded images

Access to recorded images will be restricted to the manager / supervisor who will decide whether to allow requests for access by third parties in accordance with the disclosure policy.

25.4 Viewing recorded images

Viewing of recorded images will only take place in a restricted area. Only authorised employees will have access to that area when viewing is taking place. Where possible and appropriate footage will not be viewed by the operator but will instead be downloaded and processed straight to CD/DVD in accordance with the request and only viewed by the recipient.

25.5 Operators

All operators will be trained in their responsibilities in relation to access to privacy and disclosure issues.

25.6 Removal of medium for viewing

The removal of medium on which images are recorded, for viewing purposes, will be documented in accordance with Data Protection principles and the procedure.

25.7 Access to data by third parties

Access to images by third parties will only be allowed in limited and prescribed circumstances. In the case of the Rossendale Borough Council CCTV scheme disclosure will be limited to the following:-

a) Law enforcement agencies where the images recorded would assist in a specific criminal enquiry

b) Prosecution agencies

c) Legal representatives

d) The media, where it is assessed by the Police that the public's assistance is needed in order to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. As part of that assessment the wishes of the victim of an incident should be taken into account.

e) The people whose images have been recorded and retained (Data Subject) unless disclosure to an individual would prejudice criminal enquiries or criminal proceedings.

All requests for access or for disclosure will be recorded. If access to or disclosure of the images is allowed, details will be documented.

Recorded images will not in normal circumstances be made more widely available, for example, they should not be routinely made available to the media or placed on the internet. If it is intended that the images will be made more widely available, that decision should be made by the manager or designated member of staff in accordance with the purposes of the scheme and the reason documented.

The owner should not unduly obstruct a bone fide third party investigation to verify the existence of relevant data.

The owner should not destroy data that is relevant to previous or pending search request which may become the subject of a subpoena.

The owner should decide which other agencies, if any, should have access to data and if it should be viewed live or recorded but a copy should never be made or released.

25.8 Disclosure in the public interest

Requests to view personal data that do not fall within the above categories but that may be in the public interest should be considered. Examples may include public health issues, community safety or circumstances leading to the prevention or detection of crime. Material released to a third party for the purposes of crime prevention or detection, should be governed by prior written agreement with the Chief Constable.

Material may be used for bona fide training such as Police or staff training.

25.9 Subject access disclosure

All staff involved in operating the equipment must be able to recognise a request for access to recorded images by data subjects and be aware of individuals' rights and the Council's duties set out in sections 7-9A Data Protection Act 1998.

Individuals whose images are recorded have a right to view the images of themselves and, unless they agree otherwise, to be provided with a copy of the images. Requests for such access to personal data are referred to as 'subject access requests'.

All subject access requests should be dealt with by the manager / supervisor in conjunction with the Council's legal officers.

Data subjects requesting access will be provided with a standard subject access request form to complete (Appendix 'A') and accompanying guidance notes. Although it is not compulsory for individuals to complete the request on the prescribed form, requests must be in writing and it will help to process requests efficiently and effectively if the form is completed and submitted in full. Requests can be received in hard copy or via email.

Subject access rights are governed by Section 7 of the Data Protection Act 1998 and include the following provisions:

a) A fee is paid for each search (maximum £10)

b) A person gives sufficient and accurate information about a time and place

c) Information required as to the identification of the person making the request.

d) The Data Controller only shows information relevant to the search

Individuals who make a subject access request are entitled to be:-

- Told whether any personal data is being processed
- Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- Given a copy of the personal data; and
- Given details of the source of the data (where available)

The subject access request will be dealt with promptly and in any case within 40 days of receipt of the request or within 40 days of receiving all the information required

If an individual makes a request without specifically mentioning the DPA or that it is a subject access request, or even refers to it as being a FOI request, it should still be processed as a subject access request if it is clear that the individual is asking for their own personal data.

A subject access request can be made via a third party, such as a solicitor acting on behalf of a client. In such a case the manager / supervisor will need to be satisfied that the party making the request is entitled to act on behalf of the individual, and it is the third party's responsibility to provide evidence of this, such as a written authority or general power of attorney. If the supervisor thinks that the individual may not understand what information would be disclosed to a third party who has made a subject access request on their behalf, a response may be sent directly to the individual, so that the individual can choose to share the information with the third party after having had chance to review it first.

If a subject access request is made by a child, or by a parent or guardian on behalf of a child, and the manager / supervisor is confident that the child is mature enough to understand their rights then they should respond to the child directly. In making this decision the manager / supervisor will take into account the child's level of maturity, the nature of the personal data, any consequences of allowing those with parental responsibility for the child to have access to the data, any detriment to the child if individuals with parental responsibility cannot access the information, and the

child's views about who should have access to the data. Following the approach taken in Scotland, guidance suggests that it would be reasonable to consider that a child aged 12 years or more has the capacity to make a subject access request, however the other factors should still be considered before making a decision as to who the data is disclosed to.

If a subject access request is received, it will be necessary to ascertain whether the images obtained are aimed at learning about the Data Subjects activities. If this is not the case and there has been no captured images of identifiable individuals or information relating to individuals then this may not fall within the Data Protection Act 1998 and access may be denied. Any refusal should be documented.

If on the other hand images have been obtained and CCTV used to focus on the activities of particular people either by directing cameras at an individual's activities, looking out for particular individuals or examining recorded CCTV images to find things out about the people in them such as identifying a criminal or a witness, these activities will still be covered by the DPA and reference should be made to this Code of Practice prior to the release of such data.

If images of third parties are also shown with the images of the person who has made the access request, consideration will be given as to whether there is a need to obscure the images of third parties. If providing these images would involve an unfair intrusion into the privacy of the third party, or cause unwarranted harm or distress, then they should be obscured. In many cases, images can be disclosed as there will not be such intrusion.

A search request should provide sufficient information to locate the data requested (e.g. within 30 minutes for a given date and place). If insufficient information is provided a data controller may refuse a request until sufficient information is provided.

Under certain circumstances (Section 29 of the Data Protection Act 1998) the manager or designated member of staff can decide that a subject access request is not to be complied with. In such cases the refusal will be documented.

25.10 Provision of data to the individual

The manager / supervisor having verified the validity of a request should provide requested material to the individual. Only that personal data specific to the search request should be provided. Other identifiable individuals should be blanked off by electronic screening or manual editing on the monitor screen. As there is no on site means of editing out other personal data the material would have to be sent to an editing house for processing.

The image(s) requested will be provided in a permanent 'auto-play' format (DVD) to enable it to be easily accessed by the individual.

If the individual agrees it may be possible to provide subject access by viewing only. If this is the case:

- Viewing should take place in a controlled environment
- Material not relevant to the request should be masked or edited out

Where the information is requested under the Freedom of Information Act 2000 and other people are identifiable in the CCTV pictures, the images would be considered personal information and is likely to be exempt from the Freedom of Information Act in accordance with the guidance of the Information Commissioner, and should be treated as a data protection subject access request as outlined above.

More information can be found at www.ico.gov.uk

25.11 Other rights and responsibilities

All staff involved in operating the CCTV equipment must be able to recognise a request from an individual to prevent processing likely to cause substantial and unwarranted damage to that individual.

In relation to a request to prevent processing likely to cause substantial and unwarranted damage, the manager / supervisor's response should indicate whether he or she will comply with the request or not.

The member or designated member of staff must provide a written response to the individual within 21 days of receiving the request setting out their decision on the request.

If the manager or designated member of staff decide that the request will not be complied with, they must set out their reasons in the response to the individual.

A copy of the request and response will be retained.

If such a request is received the manager / supervisor will follow guidance on this right from the Information Commissioner's Office.

25.12 Media Disclosure

Disclosure of images from the CCTV system must be controlled and consistent with the purpose for which the system was established. For example, if the system is established to help prevent and detect crime it will be appropriate to disclose images to law enforcement agencies where a crime needs to be investigated, but it would not be appropriate to disclose images of identifiable individuals to the media for entertainment purposes or place them on the internet.

Images can be released to the media for identification purposes; this will not generally be done by anyone other than a law enforcement agency.

Images, which are not required for the purpose(s) for which the equipment is being used will not be retained for longer than is necessary. As mentioned previously, on occasions images may need to be retained for longer periods as a requirement of an investigation into crime. While images are retained access to and security of the images will be controlled in accordance with the requirements of the Data Protection Act.

26. Recorded Material

Recorded material should be of high quality. In order for recorded material to be admissible in evidence total integrity and continuity must be maintained at all times.

Security measures will be taken to prevent unauthorised access to, alteration, disclosure, destruction, accidental loss or destruction of recorded material.

Recorded material will not be released to organisations outside the ownership of the system other than for training purposes or under the guidelines referred to previously.

Images retained for evidential purposes will be retained in a secure place where access is controlled.

27. Quality and Maintenance

As far as practicable efforts will be made to ensure that clear images are recorded at all times. The system will receive regular servicing and in the event of a malfunction, on discovery of a fault the supervisor will arrange for the equipment to be repaired and recording restored as soon as reasonably practicable.

All documentation relating to the equipment and its servicing and repairs is retained and will be available for inspection and audit.

28 Recordings

28.1 Digital Recordings

Records will be kept of the recorded media at all stages whilst in the owner's possession.

The record will include the following:

1) Unique equipment reference number(s);

2) Time/date/person removing medium from secure storage for use;

3) Time/date/person returning medium to secure storage after use;

4) Time and date of delivery to the law enforcement agencies, identifying the law enforcement agency officer concerned;

5) Details of all reviews of images, including persons present and results

Images will be retained for 31 days and unless containing evidence the medium will be destroyed.

Recorded material will be stored securely. Data to be destroyed will be destroyed as a controlled operation. Special consideration will be given to recorded material that has been requested by the Police or contains a known incident.

28.2 Making Recordings

Details of the recording procedures are outlined in the 'Procedure for Retrieving and Processing Requests for CCTV footage' document. Recordings will be provided in a permanent 'auto-play' format (CD / DVD) which can be easily viewed by the recipient.

Recording mediums containing original incidents will as far as possible not be replayed, unless absolutely essential to avoid any accident, damage or erasure. If recorded images need to be reviewed the reasons and details of those present will be logged and the medium returned to secure storage, if appropriate.

Rossendale Borough Council

CCTV Code of Practice

Appendix 'A'

CCTV Code of Practice

Declaration of Confidentiality

I confirm that I will treat all viewed, recorded or written material obtained from Rossendale Borough Council's CCTV system as strictly confidential and I will not divulge it to any other person, except as provided for by the Disclosure Policy contained in the Rossendale Borough Council CCTV Code of Practice.

Signed……..

Position……

Organisation……...

Dated……

Rossendale Borough Council

CCTV Code of Practice

Appendix B

Rossendalealive
BOROUGH COUNCIL

Subject Data Access Form & Guidance

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 the information in a permanent form except where the supply of such a copy is not possible or would involve disproportionate effort, or data does not fall within the Data Protection Act 1998 or if you agree otherwise. Rossendale 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 Rossendale Borough 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)

Rossendale Borough Council CCTV System Rights

Rossendale Borough Council may deny access to information where the Act allows or does not apply. 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
- Where the Data protection Act 1998 does not apply (Durant –v- FSA (2003)

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 Rossendale Borough Council. Cash will not be accepted.

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

Section 1 Asks you to give information about yourself that will help us confirm your identity. We have a duty to ensure that information it holds is ensure 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 photograph of you.

Section 3 The declaration must be signed by you.

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

The Communities Team
The Business Centre, Futures Park
Bacup OL13 0BB

SECTION 1 About Yourself

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

PLEASE USE BLOCK CAPITAL LETTERS

Title (tick box as appropriate)

Title (Mr / Miss / Mrs / Ms / Other – please state)	
Surname/family name	
First names Maiden name/former names	
Sex (please circle)	Male / Female
Height	
Date of Birth	
Place of Birth (Town & County)	
Your Current Home Address (to which we will reply)	
Post Code	
Contact Tel. No.	

If you have lived at the above address for less than 10 years, please give your previous addresses for the period: Previous address(es):	Dates of occupancy From: To: Dates of occupancy From: To:

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 license, medical card, passport or other official document that shows your name and address.

Also a recent, full face photograph of yourself.

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

SECTION 3 Supply of Information

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

(a) View the information and receive a permanent copy

YES / NO

(b) Only view the information

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:	
Print Name:	
Date:	

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

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

SECTION 5 To Help us find the Information

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

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

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

Were you:	tick box
A person reporting an offence or incident	
A witness to an offence or incident	
A victim of an offence	
A person accused or convicted of an offence	
Other – please explain	

Please confirm:	
Date(s) and time(s) of incident	
Place incident happened	
Brief details of incident	

Before returning this form

• Have you completed ALL Sections in this form?

• Have you enclosed TWO identification documents?

• Have you signed and dated the form?

• Have you enclosed the £10.00 (ten pound) fee?

Further Information:

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

The Office of the Information Commissioner,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF.
Tel. (01625) 545745

Please note that this application for access to information must be made direct to Rossendale Borough Council (address on Page 1) and NOT to the Information Commissioner.

OFFICIAL USE ONLY Please complete ALL of this Section	
Application checked and legible?	
Date Application Received	
Identification documents checked?	
Fee Paid	
Details of 2 Documents (see page 3)	
Method of Payment	
Receipt No.	
Documents Returned?	
Officer completing this Section:	
Signature	
Date	

Rossendale Borough Council

CCTV Code of Practice

Appendix C

Procedure for retrieving and processing footage

All Requests

All requests for access to CCTV footage will be directed to the Superviser and logged. The following data will be captured in order to consider and process the request:

- Date
- Name of Person requesting footage
- Requested on behalf of (if app)
- Nature of request
- Crime ref no / log no. (if app)
- Request accepted / declined (with reasons if declined)
- Camera Location
- Date & Time
- Date footage retrieved
- Date sent to person requesting / collected
- Officer

If the request is accepted in accordance with the Code of Practice, the request details, limited to the date and time and camera location, will be sent to the Operator to process. Only in circumstances where the details of the offence or offender will assist with obtaining data will additional details be supplied to the Operator.

Footage will be obtained by the appropriate method by the Operator and transferred to a CD / DVD in an auto play format. The CD / DVD will be labelled with the date, time and location of the footage by the Operator and stored securely pending collection by the person requesting the footage.

The Manager will then notify the person requesting the footage that it has been retrieved successfully and make arrangements for collection.

Equipment used for access to CCTV footage will be stored securely when not in use.

The following will be logged when accessing the footage:

1) Unique equipment reference number(s);

2) Time/date/person accessing medium;

3) Time/date/person exiting / returning medium;

4) Details of all reviews of images, including persons present and results

Electronic screening / editing

Where footage requires editing or electronic screening, the footage will be sent to an editing suite for processing with clear instructions as to what editing is required.

The Manager will be responsible for making arrangements for the editing of the footage. The person carrying out the editing will be required to sign the data confidentiality statement.

Rossendale Borough Council

CCTV Code of Practice

Appendix D

Data Protection Principles contained in Data Protection Act 1988

- *First Data Protection Principle*

"Personal Data shall be processed fairly and lawfully and in particular, shall not be processed unless :

a) At least one of the conditions in schedule 2 is met and

b) In the case of sensitive Personal Data, at least one of the conditions in schedule 3 is also met"

The above conditions are covered in the purposes for which the scheme was installed.

The definition of Personal Data and Sensitive Personal Data can be found in Section one of these codes.

- *Second Data Protection Principle*

"Personal Data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes".

- *Third Data Protection Principle*

"Personal Data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed".

- *The Fourth Data Protection Principle*

"Personal Data shall be accurate and, where necessary, kept up to date".

- *The Fifth Protection Principle*

"Personal Data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes".

- *The Sixth Data Protection Principle*

"Personal data shall be processed in accordance with the rights of data subjects under this Act".

- *The Seventh Data Protection Principle*

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

- *The Eighth Data Protection Principle*

“Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data”.