Code of Practice for the operation of Closed Circuit Television

City of York Council

In Partnership with
The Safer York Partnership
and
North Yorkshire Police

Certificate of Agreement

The content of this Code of Practice is hereby approved in respect of the City of York Closed Circuit Television System and, as far as is reasonably practicable, will be complied with by all who are involved in the management and operation of the System.

Signed for and on behalf of the City of York Council

Signature:

Name:

Position Held:

Dated:

Signed for and on behalf of North Yorkshire Police

Signature:

Name:

Position Held:

Dated:

Signed for and on behalf of the Safer York Partnership

Signature:

Name:

Position Held:

Dated:

Contents

1.0 Introduction

1.0.1 A Closed Circuit Television (CCTV) system has been introduced to the City of York. This system comprises a number of cameras installed at strategic locations.

1.0.2 Some of the cameras have pan, tilt and zoom facilities; other are fixed cameras with no 'PTZ' functionality.

1.0.3 Some cameras were primarily installed for Traffic Network Management purposes, whereas others have the primary purpose of crime prevention and detection. Many cameras serve both purposes.

1.0.4 There are currently 2 control rooms used for the operation of the system, located separately. The 'Primary Control Room' is manned 24 hours a day and is the main site for live CCTV monitoring. The second site is the 'Traffic Control Room'. It has access to the same network of cameras, but is manned infrequently.

1.0.5 At the time of writing, there are plans to co-locate the two separate control rooms.

1.0.6 All images from the camera network are first brought back to the Traffic Control Room. Here, they are all recorded 24 hours a day on a digital recording system and forwarded to the viewing stations. There are viewing stations in the Traffic Control Room and the Primary Control Room. Only the Traffic Control Room has the ability to review and retrieve past footage recorded on the digital recording system.

1.0.7 There is a single viewing station in Silver Command, Fulford Road Police Station, which will have a single video feed displayed at any one time for Police operational purposes.

1.0.8 The owner of the system is the City of York Council.

1.0.9 For the purposes of the Data Protection Act, the 'data controller' is the City of York Council, whose representative is the Assistant Director (City Strategy, Development and Transport).

1.0.10 The 'system manager' is the City of York Council, whose representative is the Head of Network Management.

1.0.11 The City of York CCTV system (hereafter referred to as 'The System') has been notified to the Information Commissioner.

1.0.12 The purpose of this Code of Practice is to describe the means by which The System shall be utilised to obtain it's stated objectives, whilst adhering to all relevant legislation pertinent to such systems.

1.0.13 Closely related to this Code of Practice is a document called the Procedural Manual. It contains detailed instructions for monitoring room operators in regards to their daily duties. It is not publicly available due to it's sensitive nature. For example, it contains instructions on how to log in to the relevant operational systems.

2.0 Key Personnel – Responsibilities and Contacts

2.0.1 System Owner:

The City of York Council is the owner of the system.

The Assistant Director (City Strategy, Development and Transport) takes on duties related to being the system owner. His role includes a responsibility to:

Ensure the provision and maintenance of all equipment forming part of The System.

Maintain close liaison with the system manager.

Ensure the operation of the system is in accordance with this Code of Practice.

Bear the duties relating to holding the position of 'Data Controller' specified in the Data Protection Act 1998

Contact:

Assistant Director – Development and Transport
City Strategy
9 St Leonards Place
York
YO1 7ET

2.0.2 System Manager:

The Head of Network Management is the manager of the system. His role includes a responsibility to:

Ensure the operation of the system is in accordance with this Code of Practice.

Maintain close liaison with the owner and operators of the system.

Make the final call regarding decisions relating to the release of footage to third parties.

Contact:

Head of Network Management
City Strategy
9 St Leonards Place
York
YO1 7ET

The Head of Network Management also has delegated responsibilities relating the Traffic Management Act 2004, details of which are referred to in section 4.7.

The system manager is also the councils designated authorisation officer in relation to the RIP Act. see section 4.6.

2.0.3 Operational Manager:

The Divisional Head of Traffic is the Operational Manager of the system. His role includes a responsibility to:

Manage the day-to-day running of the monitoring rooms, including staffing issues

Maintain close liaison with staff employed in the monitoring rooms

Contact:

Divisional Head (Traffic)
City Strategy
9 St Leonards Place
York
YO1 7ET

3.0 Purpose and Objectives of The System

3.1 *Purpose*

3.1.1 The purpose of The System, and the reasons for implementing The System are to achieve the objectives laid out below.

3.2 *Objectives*

3.2.1 To aid in the expeditious movement of traffic, as per the Traffic Management Act 2004

3.2.2 To reduce the fear of crime

3.2.3 To deter crime

3.2.4 To detect crime and provide evidential material for court proceedings

3.2.5 To assist in the overall management of the City of York

3.2.6 To enhance community safety, assist in developing the economic well being of the area and encourage greater use of the city centre and car parks

3.2.7 To assist the Local Authority in its enforcement and regulatory duties

3.2.8 To assist in Traffic Management

3.2.9 To assist in supporting civil proceedings which will help detect crime.

4.0 Privacy and Relevant Legislation

4.1 *Legality of The System*

4.1.1 Section 163 of the Criminal Justice and Public Order Act 1994 creates the power for local authorities to provide closed circuit television coverage of any land within their area for the purposes of crime prevention or victim welfare and it is also considered a necessary initiative by the police towards their duty under the Crime and Disorder Act 1998.

4.2 *Data Protection Act 1998*

4.2.1 The Act is freely available from The Office of Public Sector Information at www.opsi.gov.uk - It is too large to reproduce here in full but will be referred to throughout.

4.2.2 Concern over the use of public space CCTV systems has become a topic of much discussion in recent years. Concern typically centres on the two issues of personal privacy and how recorded images of oneself are to be utilised.

4.2.3 With the growing use of such systems, it was deemed that public confidence could only be maintained by tighter legislation covering their usage and deployment (House of Lords Select Committee on Science and Technology – 5th Report – Digital Images as Evidence)

4.2.4 This legislation took the form of the Data Protection Act 1998. This act is built upon the 1984 Act, broadening its definitions such that it can more effectively be applied to CCTV systems. It is this 1998 Act that provides much of the legal framework by which the City of York Council is obligated to operate The System.

4.2.5 All personal data obtained by 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, those objectives having been specified in section 3.2. In processing personal data there will be total respect for everyone's right to respect for his or her private and family life and their home. The process by which this shall be achieved is specified in section 8.0.

4.2.6 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. These processes are specified in section 8.0.

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

4.2.8 All data will be processed in accordance with the principles of the Data Protection Act, 1998 which are summarised below:

i) All personal data will be obtained and processed fairly and lawfully.

ii) Personal data will be held only for the purposes specified.

iii) Personal data will be used only for the purposes, and disclosed only to the people, shown within these codes of practice.

iv) Only personal data will be held which are adequate, relevant and not excessive in relation to the purpose for which the data are held.

v) Steps will be taken to ensure that personal data are accurate and where necessary, kept up to date.

vi) Personal data will be held for no longer than is necessary.

vii) Individuals will be allowed access to information held about them and, where appropriate, permitted to correct or erase it.

4.3 ***Subject Access Request***

4.3.1 A guide relating to the Councils policy for producing footage captured by The System is located in the appendices. The guide should be your first reference when discovering whether you will be able to access data held on The System.

4.3.2 Note: Each and every application for release of footage will be assessed on its own merits and general 'blanket exemptions' will not be applied.

4.3.3 The Council's policy for footage release takes into account one's rights as laid out in the Data Protection Act 1998 (namely requests for information under Section 7, the Data Subject Access legislation) Laid out below is information regarding requests that fall into this category.

4.3.4 Any request from an individual for the disclosure of personal data which he / she believes is recorded by virtue of the system will be directed in the first instance to the system manager.

4.3.5 The principles of Sections 7 and 8, and 10 of the Data Protection Act 1998 (Rights of Data Subjects and Others) shall be followed in respect of every request.

4.3.6 Any person making a request must be able to satisfactorily prove their identity and provide sufficient information to enable the data to be located. The appropriate 'Subject Access' request form is in the appendices.

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

Personal data processed for any of the following purposes -

i) the prevention or detection of crime

ii) the apprehension or prosecution of offenders

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

4.3.9 Further information on retrieving recorded material under this legislation is in section 11.4.

4.4 ***The Human Rights Act 1998***

4.4.1 The Act is freely available from The Office of Public Sector Information at www.opsi.gov.uk - It is too large to reproduce here in full but will be referred to throughout.

4.4.2 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 York is a necessary, proportionate and suitable tool to help reduce crime, reduce the fear of crime and improve public safety.

4.4.3 It is recognised that operation of the City of York CCTV System may be considered to infringe on the privacy of individuals. The partnership recognise that it is their responsibility to ensure that the system should always comply with all relevant legislation, to ensure its legality and legitimacy.

4.4.4 The system will only be used as a proportional 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, the economic well being of the area (for example, aiding the expeditious movement of traffic), for the prevention and detection of crime or disorder, for the protection of health and morals or for the protection of the rights and freedoms of others.

4.4.5 The Code of Practice and 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 free trial.

4.4.6 The City of York CCTV System shall be operated with respect for all individuals, recognising the right to be free from inhumane or degrading treatment and avoiding discrimination on any grounds 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.

4.5 ***Freedom of Information Act 2000***

4.5.1 The Act is freely available from The Office of Public Sector Information at www.opsi.gov.uk - It is too large to reproduce here in full but will be referred to throughout.

4.5.2 The Freedom of Information Act 2000 gives the public a general right of access to information held by local authorities to promote openness and accountability.

4.5.3 This act may be used to request specific information about the operation of The System.

4.5.4 Due to its sensitive nature, recorded material collected by The System is not available under this act, confidential information being an example of material exempt from the act. Individuals are advised to seek access via the Data Subject Access legislation in the Data Protection Act 1998 if they require access to recorded material.

4.6 ***Regulation of Investigatory Powers Act 2000***

4.6.1 The Act is freely available from The Office of Public Sector Information at www.opsi.gov.uk - It is too large to reproduce here in full but will be referred to throughout.

4.6.2 The Regulation of Investigatory Powers Act 2000 was introduced to regulate surveillance and similar activities carried out by public bodies.

4.6.3 The system manager, named in section 2.0, is the councils authorising officer in relation to the RIP Act.

4.6.4 The CCTV operators shall be trained to identify surveillance that requires RIP Act authorisation and know the process required to obtain this authorisation. Surveillance requiring such authorisation shall not be carried out without obtaining authorisation. Certain instances may necessitate retrospective authorisation.

4.6.5 The Act defines 2 types of covert surveillance relevant to the use of CCTV systems, 'intrusive' and 'directed' surveillance. The following paragraphs refer to The Acts definition of 'directed' and 'intrusive'.

4.6.6 Intrusive surveillance shall only be undertaken at the request of the police or similar body, and only then on receipt of RIP Act authorisation from a suitable officer, examples named in The Act.

4.6.7 Directed surveillance shall primarily be carried out at the request of the police or similar body, though the council retains it rights under The Act to authorise directed surveillance in certain necessary instances.

4.6.8 To maintain public confidence in The System, The council pledges not use directed surveillance for minor or petty offences and shall only resort to directed surveillance in significant cases where other solutions have been exhausted.

4.6.9 An example where directed surveillance shall not be employed would be in determining the school catchment area of residents for purposes of determining an school applicants validity.

4.6.10 An example where directed surveillance would be permitted would be to determine the identity of individuals engaged in repeated criminal damage to property with the aim of bringing about a prosecution.

4.7 ***Traffic Management Act 2004***

4.7.1 The City of York Council has a responsibility under the Traffic Management Act 2004 to 'secure the expeditious movement of traffic on the authority's road network'

4.7.2 Under this act, the Council must name a 'Traffic Manager' who holds accountability for undertaking said responsibilities. The Traffic Manager for the City of York is the Head of Network Management as shown in section 2.0. The Head of Network Management thus has a dual role as CCTV System Manager and Traffic Manager.

4.7.3 The council undertakes it's duties as per TM Act 2004 via several means, an integral tool to these being the use of The System. As per section 3.2, purpose 3.2.1 of The System derives its necessity from this act.

4.7.4 No such operation of The System for Traffic Management duties will fall outside the rules applied to the operation of the system for other purposes.

4.7.5 As such, this Code of Practice; any guidance, rules or obligations; restraints or policies, shall be followed equally whether The System be used for Traffic Management duties, or for prevention/detection of crime and disorder. This includes, but is not limited to obligation under Freedom of Information and Data Protection Acts.

5.0 Camera Installation and Coverage

5.1 *Installation*

5.1.1 The siting of new camera installations will be considered carefully, so as to comply with all relevant legislation, particularly the Data Protection Act 1998.

5.1.2 Consideration shall be given to the fact that a cameras location will be chosen such that it is capable of carrying out the purpose for which it was installed.

5.1.3 From time to time transportable or mobile cameras may be temporarily sited within the area. The use of such cameras, and the data produced by virtue of their use, will always accord with the objectives of the CCTV System and be governed by these Codes and Procedures.

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

5.1.5 All permanent camera locations will be advertised by the siting of appropriate signs, visible upon entering the area for which the camera covers.

5.2 *Coverage*

5.2.1 Cameras should be sited such that they can only monitor areas that are intended to be covered.

5.2.2 In those instances where the previous proviso cannot be complied with, installation can still go ahead, but consideration must be given to the procedures involved with coverage of areas not intended to be viewed.

5.2.3 In those instances where it is not possible to restrict coverage of areas not intended to be viewed, the operators will comply with their training in regards to recognising the privacy implications of such spaces being monitored (First and Third Data Protection Principles)

5.2.4 There are instances where coverage of private property may be necessary. These instances are described and governed under the section covering the Regulation of Investigatory Powers Act 2000, section 4.6.

6.0 Monitoring Rooms – Access, Security, Staffing and Facilities

6.1 *Access*

6.1.1 Only authorised persons will be permitted access to the CCTV monitoring rooms.

6.1.2 Appendix C lists the persons with pre-approved authorisation for access to the monitoring rooms.

6.1.3 Authorisation for persons not on the pre-approval list will be at the System Managers discretion.

6.1.4 Public access will normally be prohibited.

6.1.5 All persons accessing the monitoring rooms will be required to fill in the access control log, part of which is a visitors declaration of confidentiality, located in Appendix D.

6.2 *Security*

6.2.1 A trained and authorised operator must be present at all times when the equipment is in use. If the monitoring facility is to be left unattended for any reason it will be secured. In the event of the monitoring room having to be evacuated for safety or security reasons, the provisions of the Procedural Manual will be complied with.

6.2.2 In the event that a Lay Visitor (section 9.1) or approved visitor (within the terms outlined in section 6.1.3) is present within the monitoring room, all cameras shall be operated only in wide angle and in such a manner that the identification of individuals or specific vehicles is not possible.

6.2.3 The monitoring rooms will at all times be secured by a locked door. This door is to remain closed and locked at all times other than for access of authorised personnel.

6.2.4 It is the responsibility of any authorised operator to ensure that the above access requirements are complied with at all times. Should any operator find that the monitoring room or its equipment has been left insecure the operator shall secure the equipment appropriately and an immediate report of the incident, quoting the time and date must be made to the system manager within 24hrs.

6.3 *Staffing*

6.3.1 The Operational Manager is responsible for managing the staffing of the monitoring rooms.

6.3.2 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.

6.3.3 Operators will all be SIA trained and licensed.

6.3.4 Every person involved in the management and operation of the system will be personally issued with a copy of both the Code of Practice and the Procedural Manual, will be required to sign a confirmation that they fully understand the obligations adherence to these documents places upon them and that any breach will be considered as a disciplinary offence. They will be fully conversant with the contents of both documents, which may be updated from time to time, and which he / she will be expected to comply with as far as is reasonably practicable at all times.

6.3.5 All operators shall receive training relevant to their role in the requirements of the Human Rights Act 1998, Data Protection Act 1998, Regulation of Investigatory Powers Act 2000 and the Codes of Practice and Procedures. Further training will be provided as necessary.

6.4 ***Discipline***

6.4.1 Every individual with any responsibility under the terms of this Code of Practice and who has any involvement with The System to which they refer, will be subject to the Employing Authority discipline code. Any breach of this Code of Practice or of any aspect of confidentiality will be dealt with in accordance with those discipline rules.

6.4.2 The system manager will accept primary responsibility for ensuring there is no breach of security and that the Code of Practice is complied with. The system manager will have day to day responsibility for the management of the monitoring room and for enforcing the discipline rules. Non-compliance with this Code of Practice by any person will be considered a severe breach of discipline and dealt with accordingly including, if appropriate, the instigation of criminal proceedings.

6.4.3 Every individual with any responsibility under the terms of this Code of Practice and who has any involvement with The System to which they refer, will be required to sign the operators declaration of confidentiality. This document is located in Appendix E

6.5 ***Facilities***

6.5.1 A staffed monitoring room is located at Police Divisional Headquarters, Fulford Road, York (The Primary Control Room)

6.5.2 The Primary Control Room has no recording facilities housed in it. All footage viewed from the Primary Control Room is automatically recorded at the Secondary Control Room.

6.5.3 The Primary Control Room has access to the Police 'Airwave' Radio system.

6.5.4 The Secondary Control Room is located in the UTC room (Traffic Control Room) at the Council Headquarters. It has access to exactly the same network of cameras as the Primary Control Room. It is manned only during office hours.

6.5.5 The Secondary Control Room houses all recording facilities for both Primary and Secondary control rooms. It also houses the facilities necessary for viewing and managing the recorded material and appropriately processing requests for footage.

7.0 System Operation Practice

7.0.1 This section covers those non-sensitive general practices involved in the operation of the system, in either control room.

7.0.2 Participation in the system by any organisation, individual or authority assumes an agreement by all such participants to comply fully with this Code and to be accountable under the Code of Practice.

7.1 *Operation Principles*

7.1.1 Any person operating the cameras will act with utmost probity at all times.

7.1.2 The system will be operated in accordance with the Data Protection Act at all times. Further detail can be found in section 4.2.

7.1.3 The system will be operated in accordance with all the requirements and the principles of the Human Rights Act 1998. Further detail can be found in section 4.4.

7.1.4 Camera operators will be mindful of exercising prejudices which may lead to complaints of the system being used for purposes other than those for which it is intended. The operators may be required to justify their interest in, or recording of, any particular individual, group of individuals or property at any time by virtue of an audit of the system.

7.1.5 The system will be operated with due regard to the principle that everyone has the right to respect for his or her private and family life and their home.

7.1.6 The public interest in the operation of the system will be recognised by ensuring the security and integrity of operational procedures. This Code of Practice contains the means by which this shall be achieved.

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

7.2 *Operation Practice*

7.2.1 As previously stated in section 1.0.13, "Closely related to this Code of Practice is a document called the Procedural Manual. It contains detailed instructions for monitoring room operators in regards to their daily duties. It is not publicly available due to its sensitive nature. For example, it contains instructions on how to log in to the relevant operational systems."

7.2.2 The cameras, control equipment, recording and reviewing equipment shall at all times only be operated by persons who have been trained in their use and the legislative implications of their use.

7.2.3 Every use of the cameras will accord with the purposes and key objectives of the system and shall be in compliance with this Code of Practice.

7.2.4 Cameras will not be used to look into private residential property except under specific circumstances. This highly regulated behaviour is explained and described in section 4.6 and section 10.3.

7.2.5 The operation of the system will also recognise the need for formal authorisation of any covert 'Directed' surveillance or crime – trend (hotspot') surveillance as required by the Regulation of Investigatory Powers Act 2000 (RIP Act), further info in section 4.6.

7.2.6 The System will be operated fairly, within the law, and only for the purposes for which it was established and are identified within this Code, or which are subsequently agreed to be in accordance with this Code of Practice.

7.3 ***Control Priority***

7.3.1 Operators located in the Primary Control Room have priority in operation of any of the cameras on the System. This priority is due to the fact that the Primary Control Room has access to the Police 'Airwave' Radio system, giving them a better idea of what incidents require the most immediate attention.

7.3.2 This priority is achieved by programming built into the system whereby simultaneous operation of a camera by both the Primary and Secondary control rooms will default to taking commands from only the Primary control room.

7.3.3 The operators in the Primary Control Room have the ability to choose which camera is displayed on the monitor in Silver Command. The choice of camera shown will usually be at the request of the Police.

7.4 ***Incident Logging***

7.4.1 Whenever an operator witnesses a incident, he shall note down the relevant details in the incident log at his control station.

7.4.2 Each incident will be sequentially numbered, dated and timed.

7.4.3 Any incident or circumstance which gives rise to suspicion or concern even if no further action is required by North Yorkshire Police should be recorded in the incident log.

7.5 ***Directed Surveillance Requests***

7.5.1 There will be occasions upon which the Police not only request a specific camera be shown in Silver Command, but that the camera be operated in a way that constitutes 'Directed Surveillance'.

7.5.2 All operators will be able to identify requests that fall under the category of 'Directed Surveillance' and will know the action to take in regards to the Regulation of Investigatory Powers Act 2000 (RIP Act). More information on the RIP Act is in section 4.6.

7.5.3 A record of any request is to be made into a book specifically held for this purpose after the operator has satisfied him/herself that the request falls within a category for which directed surveillance may be considered appropriate under the RIP Act.

7.5.4 Each request will be sequentially numbered, dated and timed and the record endorsed with the name and number of the police officer requesting the directed surveillance and brief details of the reason for the request. The time that the directed surveillance ceased shall also be entered into the record.

7.5.5 Directed surveillance requests from sources other than the police will only be accepted upon written authorisation by The System Owner. Upon such authorisation being given, the above information will be entered into the Directed Surveillance record book. In any case, section 4.6 still applies.

7.6 ***Operational Command of the System by the Police***

7.6.1 Under rare and extreme operational circumstances the Police may make a request to command the use of The System to which this Code of Practice applies. These circumstances may be a major incident or event that has a significant impact on the prevention and detection of crime or public safety. Such use will provide the police with a broad overview of events in order to command the incident.

7.6.2 Such requests will be viewed separately to the use of the systems' cameras with regard to the requirement for an authority for specific types of surveillance under the Regulation of Investigatory Powers Act 2000

7.6.3 Applications made as at section 7.6.1 will be considered on the written request of a police officer not below the rank of Superintendent. Any such request will only be accommodated upon the personal written permission of the most senior representative of the System owners, or designated deputy of equal standing. In the event of an urgent need, a verbal request of the senior officer in charge, and in any case an officer not below the rank of Inspector, will be necessary. This should be followed as soon as practicable within 72 hours by a Superintendents' written request.

7.6.4 In the event of such a request being permitted, the Monitoring Room will continue to be staffed, and equipment operated by, only those personnel who are specifically trained to do so, and who fall within the terms of Appendix C of this Code. They will then operate under the command of the police officer designated in the verbal / written request, taking into account their responsibilities under this code.

7.6.5 In very extreme circumstances a request may be made for the Police to take total control of The System in its entirety, including the staffing of the monitoring room and personal control of all associated equipment, to the exclusion of all representatives of the System owners. Any such request should be made to The

system manager in the first instance, who will consult personally with the most senior officer of the system owners (or designated deputy of equal standing). A request for total exclusive control must be made in writing by a police officer not below the rank of Assistant Chief Constable or person of equal standing.

7.7 ***Maintenance of the System***

7.7.1 To ensure compliance with the Information Commissioners Code of Practice and that images recorded continue to be of appropriate evidential quality The System shall be maintained in accordance with the requirements laid out below.

7.7.2 The maintenance agreement will make provision for regular/ periodic service checks on the equipment which will include cleaning of any all weather domes or housings, checks on the functioning of the equipment, and any minor adjustments that need to be made to the equipment settings to maintain picture quality.

7.7.3 The maintenance will also include regular periodic overhaul of all the equipment and replacement of equipment which is reaching the end of its serviceable life.

7.7.4 The maintenance agreement will also provide for 'emergency' attendance by a specialist CCTV engineer on site to rectify any loss or severe degradation of image or camera control.

7.7.5 The maintenance agreement will define the maximum periods of time permitted for attendance by the engineer and for rectification of the problem depending upon the severity of the event and the operational requirements of that element of the system.

7.7.6 It is the responsibility of the System Manager to ensure appropriate records are maintained in respect of the functioning of the cameras and the response of the maintenance organisation.

8.0 Management of Recorded Material

8.1 *Principles*

8.1.1 For the purpose of this Code of Practice, 'Recorded Material' refers to any digital images stored by any part of The System. A single digital image may be referred to as a video 'still' or 'print' but differs from video footage only in the fact that a still is a single image whereas a video comprises of a number of sequential images.

8.1.2 The System is only capable of recording digital images; no videotape functionality is present.

8.1.3 There are only 2 ways in which The System can store recorded material. The first is within an isolated storage device located in the camera to which it is attached. The second is by means of a centrally located storage device at the Secondary Control Room which concurrently records all cameras connected to it. Cameras linked to the centrally located storage device comprise the majority of The Systems camera estate and are referred to as 'fibre' cameras due to the communications method employed.

8.1.4 Both means of recording shall be treated the same in regards to the management of recorded material stored thereupon.

8.1.5 Access to and the use of recorded material will be strictly for the purposes defined in this Code of Practice only.

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

8.1.7 The practice laid out below in regards to managing recorded material is devised as to comply with the Data Protection Act 1998 and the Information Commissioners Code of Practice. Specifically, those parts relating to the storage of personal data (Data protection Principles 4, 5 and 7)

8.2 *Practice*

8.3 Retention - Images shall be retained for 31 days, after which they will be automatically overwritten, unless backed up on a separate device or media. 31 days has been chosen as the retention period due to a compromise between the technological storage capabilities of current technology, against the period of time it can take for criminal activity to be reported. (See Data Protection Principle 5)

8.4 Quality – Footage from every fibre camera is recorded 24 hours a day in the Secondary Control Room. The quality of footage varies from camera to camera, but in any case will not typically fall below 10fps at 704x576. As stated, this quality of footage will be maintained for 31 days, 24 hours a day when no faults are present.

8.4.1 The system is capable of recording at higher framerates and resolutions, but this quality and framerate has been calculated such that evidential quality footage is still available, yet there is not an unreasonable demand upon storage resources.

8.5 Spot Recording – As a means of replacing conventional videotape 'spot recording' facilities, a process has been set up on the central storage device to provide extra short-term, high quality recording for every camera, as a supplement to the standard quality long-term footage. For a period of 168 hours, footage from every camera shall also be recoded in 24fps at maximum possible resolution. The operators must then ensure the 'best evidence' is removed from the system where possible by organising the retrieval of footage within the stated period. It is to be noted and expected that in a lot of cases, the report of an incident will be received after the 'spot recording' footage has expired, and only the standard quality of footage will be available.

8.6 Viewing – Recorded material shall only be viewed by authorised operators and only in a private, secure location. This will be the Secondary Control Room. Viewings by third parties will be at the discretion of the system manager as per the procedures in sections 6.0 and 11.0 and 4.2. (7th data Protection Principle)

8.7 Removal - Recorded material removed from The System will remain in digital format, on a CD, DVD or Hard Disk Drive. The removal of footage shall be documented in the following way.

8.7.1 A CD / DVD / HDD production log is held within the Secondary Control Room and is filled in for EVERY instance in which recorded material is removed from The System.

8.7.2 The log documents:

The date on which the images were removed from the system
The date and time/period of the footage removed
The camera(s) the footage was removed from
The location the footage pertains to
A crime reference number if relevant
The incident to which the footage relates
The operator who removed the footage
The operator who handed the footage over to the third party
The third party who is in receipt of the footage
The date and time the footage was handed over

8.7.3 This procedure complies with and exceeds the requirements of the 3rd and 7th Data Protection Principles.

8.7.4 The security of stored recorded material is addressed as follows

8.7.5 Recorded material stored on the centrally located storage device is secured by means of being located in a restricted room (see section 6.2) and by means of a password protected viewing station.

8.7.6 Material produced to CD / DVD / HDD is secured by means of being located in the restricted room until being removed by a third party who signs the production log, documenting its removal. Once removed, the third party becomes responsible for it's security.

8.7.7 These measures satisfy the 5th and 7th Data Protection Principles.

8.7.8 Requests for footage from third parties, including Data Subject Access Requests are explained in section 11.0.

9.0 Assessment of The System

9.0.1 Assessment of The System can take many forms, from cost benefit analyses as to it's cost effectiveness, to enquiries into whether The System is being operated within this Code of Practice, and hence legally. Other forms of assessment may also become necessary over the course of the life of The System.

9.0.2 The primary means by which The System facilitates assessment is via a comprehensive audit trail covering all aspects of its operation. An assessment can be carried out at any point due to the data that is always available on the following topics, from the mentioned sources.

9.0.3 Note that the following information may be construed as sensitive and will not necessarily be available under the Freedom of Information Act.

9.0.4 Financial Implications – The System is financed from specific budgets in the City of York Council. As such, The Council's Financial Management System has a complete record of all expenditure on The System.

9.0.5 Impact upon Crime – The Police have access to crime statistics for areas covered by The System.

9.0.6 Additionally, a record is kept of every evidential piece of footage that is provided to the Police, with relevant incident number and evidence tag. Amongst other forms of analyses, one possible process is for the Police, on receipt of this record, to determine how many pieces of surrendered footage have been used in court proceedings.

9.0.7 Legal operation of The System – As stated in section 8.0, every movement and production of footage shall be recorded, this enables an assessment of whether Recorded Material has been managed legally and in accordance with this Code of Practice.

9.0.8 Every usage of any camera attached to The System is recorded on the centrally located recording facility. An assessment of direct usage of cameras in line with the law and this Code of practice can be enacted from this recorded material.

9.0.9 Utility for Traffic Management and City Centre Administration – A log shall be kept of all uses of The System for Traffic Management and City centre Administration purposes.

9.0.10 These audit trails provide sufficient evidence to assist in any assessment of The System.

9.1 *Lay Visitor Scheme*

9.1.1 Regular assessments are carried out by a group of lay visitors who visit the control rooms to determine whether The System is being operated in accordance with this Code of Practice. The Lay visitor scheme operates as follows.

9.1.2 The lay visitors panel shall consist of 10 people who can apply for the positions when advertised.

9.1.3 Exclusions from applications:

- Officers of local government or their immediate families
- Police officers.
- Elected members of local or national government.
- Applicants with a criminal record.

9.1.4 All applications will be subject to vetting by the police.

9.1.5 Application will be forwarded to the chairman of the local Community and Police Group for interview and selection. This recommendation will then be forwarded to the Police Authority for confirmation.

9.1.6 Positions will be held for two and three years initially and thereafter every two years.

9.1.7 The lay visitors will be responsible for undertaking an ethical and procedural audit to ensure the code of practice is being complied with and will submit an annual report to the City of York Council and the Chief Constable.

9.2 ***Changes to the Code of Practice or Procedural Manual***

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

9.2.2 A minor change, (i.e. such as may be required for clarification and will not have such a significant impact) may be agreed between the manager and the owners of the system.

10.0 Accountability and Public Information

10.1 *Overall Accountability*

10.1.1 The Assistant Director (City Strategy, Development and Transport), named in section 2.0.1, being the nominated representative of the system owners, bears duties relating to being the owner of The System.

10.1.2 Formal consultation will take place between the owners and the managers of the system with regard to all aspects, including this Code of Practice and the Procedural Manual.

10.1.3 The other parties with responsibilities relating to The System are listed in section 2.0.

10.2 *Accountability in regards to observing incidents*

10.2.1 The presence of a CCTV system does not guarantee that every action in the vicinity of a camera will be captured. This is due to the uni-directional nature of cameras, the limits upon the resolution of images captured by cameras; and infrequent, unavoidable hardware failures.

10.2.2 Furthermore, the number of cameras available exceeds the number of operators, meaning it is not possible to monitor every camera continuously.

10.2.3 Taking these points into consideration, the City of York Council will not be held accountable for failure to observe any incidents occurring in the vicinity of cameras.

10.3 *Public Information*

10.3.1 A copy of this Code of Practice shall be published on the City Councils' web site, and a copy will be made available to anyone on request. Additional copies will be lodged at public libraries, local police stations and Council 'receptions. Salient details of this Code of Practice will also be made available in leaflet form.

10.3.2 Signs will be placed in the locality of the cameras and at main entrance points to the relevant area. The signs will indicate:

i) The presence of CCTV monitoring;

ii) The 'ownership' of the system;

iii) Contact telephone number of the 'data controller' of the system.

10.3.3 The system will be subject to audit by an independent volunteer group of lay visitors, see section 9.1.

10.3.4 Cameras capable of obtaining personal information from private property will not be used to do so except under the specific requirements of an RIP Act request. See section 4.6. Furthermore, such an RIP Act request will only be made for investigations originating from the police or other body investigating serious

offences. Minor and non-criminal offences will not be investigated using intrusive surveillance.

10.3.5 An example for which intrusive surveillance will be used would be the monitoring of a private property being the focus of a police drugs raid or hostage situation.

10.3.6 All CCTV staff are contractually subject to regulations governing confidentiality and discipline. An individual who suffers damage or distress by reason of any contravention of this Code of Practice may be entitled to compensation.

10.4 ***Complaints***

10.4.1 A member of the public wishing to register a complaint with regard to any aspect of The System may do so by contacting the System Owners representative – The Assistant Director (Development and Transport). All complaints shall be dealt with in accordance with the City of York Councils' complaints procedure, a copy of which may be obtained from the Guildhall, York or any Council offices. Any performance issues identified will be considered under the organisations disciplinary procedures to which all members of the City of York Council, including CCTV personnel are subject.

11.0 Release of footage to Third Parties

11.0.1 This section details the principles and procedures involved with the release of footage captured by The System. Located in Appendix A is a guide that will provide an indication on whether footage will be produced for any particular situation. Note that each individual request is still considered on it's own merit.

11.1 *Principles*

11.1.1 Disclosure of recorded material to Third Parties will be made only under the circumstances laid out in this Code of Practice.

11.1.2 Requests for access to recorded material shall be recorded.

11.1.3 Every request for the release of personal data generated by this CCTV System will be channelled through the System Manager. The System Manager will ensure the principles contained within this Code of Practice are followed at all times.

11.1.4 Recorded material shall be processed lawfully and fairly and used only for the purposes defined in the Code of Practice

11.1.5 The release or disclosure of data for commercial or entertainment purposes is specifically prohibited

11.1.6 The City of York Council and its partners are committed to the belief that everyone has the right to respect for his or her private and family life and their home.

11.2 *Police Requests for Release of Footage*

11.2.1 The majority of requests received by The Council relating to the release of footage come from The Police. As such, a streamlined process has been established that ensures footage is released in accordance with all relevant legislation, as expediently as possible.

11.2.2 This process applies not only to the civil police, but also to: Immigration or Customs Officers, Port Authority or Coastguard Officers, HSE Officers, Fire or Ambulance Officers, British Transport Police Officers, Ministry of Defence Officers, Military Police Officer, Civil Nuclear Constabulary, National Security Service. For brevity, only 'The Police' shall be mentioned hereafter.

11.2.3 The request must relate to one of the following lawful purposes:

- Providing evidence in criminal proceedings
- The prevention of crime
- The investigation and detection of crime
- Identification of witnesses

11.2.4 These purposes being deemed lawful as they coincide with the named purposes of The System, and these purposes being legitimate due to the Police and Criminal Evidence

Act 1984 and Criminal Procedures and Investigations Act 1996 (amongst others), thus satisfying the First Data Protection Principle.

11.2.5 The Police must provide satisfaction that any request made is for one of the above aforementioned lawful purposes. This will usually take the form of a crime reference number relating to the incident in question that will be recorded with the details of the request.

11.3 ***Secondary Requests for Release of Footage***

11.3.1 A Secondary request can be thought of as a request that does not originate from the Police and also does not fall under a Data Subject Access Request (see section 11.4). Examples of Secondary requests would be from the media and solicitors.

11.3.2 Each secondary request will be individually considered by referring to The Councils Policy on Release of Footage to Third Parties (Appendix A)

11.3.3 Consideration will also be given to ensure that complying with the request would not contravene any relevant legislation, eg. Data Protection Act 1998, Human Rights Act 1998, Criminal Justice and Public Order Act 1994.

11.3.4 Consideration of any known case law will also be taken into account.

11.3.5 Consideration will be given as to whether release of footage would pass a test of 'disclosure in the public interest'.

11.3.6 The final decision as to whether footage shall be disclosed to a third party will come from the System Manager.

11.4 ***Data Subject Access Request***

11.4.1 Section 7 of The Data Protection Act 1998 gives provision to individuals to request access to information held about themselves.

11.4.2 This provision means that a person may make a request to the system manager to view footage of themselves captured by The System.

11.4.3 A person making a request to review footage of themselves can do so through the form located in Appendix B.

11.4.4 There is a charge of £10 for each request made.

11.4.5 The system manager is not obliged to comply with a request under this section unless he is supplied with such information as he may reasonably require in order to satisfy himself as to the identity of the person making the request and to locate the information which that person seeks.

11.4.6 Where a system manager cannot comply with the request without disclosing information relating to another individual who can be identified from that information, he is not obliged to comply with the request unless:

- the other individual has consented to the disclosure of the information to the person making the request, or
- it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

11.4.7 In determining 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,
- any steps taken by the data controller with a view to seeking the consent of the other individual,
- whether the other individual is capable of giving consent, and
- any express refusal of consent by the other individual.

11.5 ***Control of recorded material after release***

11.5.1 Copyright on the footage contained on any released recorded material stays with the City of York Council. All laws pertaining to the usage of copyrighted material apply.

11.5.2 Persons receiving recorded material must also sign an agreement laying out the terms by which they accept receipt of said material, and the terms under which the material may be used.

11.5.3 If the City of York Council incurs damage due to use of released footage outside of the signed agreement, the City of York Council may seek recompense from the party in breach of aforementioned agreement.

11.5.4 Responsibility for controlling released footage in accordance with said agreement falls with the third party to who the material was released.

11.5.5 Should the third party, at a point in the future, no longer feel capable of honouring the agreement, the recorded material will be destroyed.

Appendix A

Policy for release of footage to Third Parties

This section gives a quick reference as to the Council's policy on release of recorded material to third parties. Each request will be considered on it's own merits, and in accordance with the relevant legislation, however this section covers the majority of instances that arise.

Release of footage may be predicated by the acceptance of terms of use by the third party.

Third Party:	Police Officer / Immigration or Customs Officer / Port Authority or Coastguard Officer / HSE Officer / Fire or Ambulance Officer / British Transport Police Officer / Ministry of Defence Officer / Military Police Officer / Civil Nuclear Constabulary / National Security Service
Policy:	Footage produced on provision of incident number and other necessary information.

Third Party:	Media / Media representative
Policy:	Footage is not to be released to the media for entertainment purposes. Footage for purposes such as advertising missing persons should be received from the police, with the councils consent.

Third Party:	Insurer
Policy:	Is the request in relation to an Insured's claim? If No, Go to 1 If Yes, Go to 2
1	Request refused.
2	Footage usually produced. The council will first evaluate the footage to determine whether production would be in contravention of any relevant legislation.

Third Party:	Solicitor
Policy:	Is the request in relation to Civil Proceedings? If No, Go to 1 If Yes, Go to 2
1	Request Refused. Footage relating to criminal proceedings will always be channelled through the Police.
2	Request usually accepted. The council will review the footage to determine whether production would be in contravention of any relevant legislation. In some circumstances, a court order or subpoena may be required.

Third Party:	Individual
Policy:	Are you requesting footage of yourself? If No, Go to 1 If Yes, Go to 2
1	Request Refused. Data Protection Act - Section 7 – Data Subject Access Request is the primary process for individuals requesting recorded material.
2	Is the request in relation to a crime or criminal activity alleged to be committed by yourself or somebody else? If Yes, Go to 3 If No, Go to 4
3	Request Refused. Footage relating to potential criminal incidents must be channelled through the Police.
4	Is the request in relation to an insurance claim? If Yes, Go to 5 If No, Go to 6
5	Refuse Request. Footage relating to insurance claims is provided direct to insurance companies upon request from the insurance company.
6	Is the request in relation to civil proceedings? If Yes, Go to 7 If No, Go to 8
7	Refuse Request. Footage relating to civil proceedings is provided direct to solicitors upon request from a solicitor.
8	Request considered under Data Protection Act 1998, fill in form at Appendix B for consideration.

Appendix B

Data Subject Access Request Form

How to Apply For Access To Information Held On the CCTV System

These notes explain how you can find out what information, if any, is held about you on the CCTV System. They also explain how to request copies of such information. Requests will be denied if you do not provide sufficient detail to enable the relevant information of yourself to be found.

Your Rights

Subject to certain exemptions, you have a right to be told whether any personal data is held about you. You also have a right to a copy of that information in a permanent form except where the supply of such a copy is not possible or would involve disproportionate effort, or if you agree otherwise. The City of York Council will only give that information if it is satisfied as to your identity. If release of the information will disclose information relating to another individual(s), who can be identified from that information, the Council is not obliged to comply with an access request unless –

- The other individual has consented to the disclosure of information
- It is reasonable to comply with the request without the consent of the other individual(s)
- It is possible and reasonable to edit out such information

The City of York System Owners Rights

The City of York Council may deny access to information where the Act allows. The main exemptions in relation to information held on the CCTV System are where supplying the information may jeopardise the enactment of:

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

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 **'The City of York Council '**.

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

Section 1	Asks you to give information about yourself that will help the Council to confirm your identity. The City of York Council has a duty to ensure that information it holds is secure and it must be satisfied that you are who you say you are.
Section 2	Asks you to provide evidence of your identity sufficient to enable a search of your stored data. This will take the form of photo-identification documents.
Section 3	Asks you to confirm whether you will accept just viewing the information, or if you want a copy of the information.
Section 4	**You must sign the declaration**

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

The Head of Network Management, The City of York Council, 9 St Leonards Place, York , YO1 2ET .

If you have any queries regarding this form, or your application, please ring the Head of Network Management on (01904) 551414

SECTION 1 About Yourself

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

PLEASE USE BLOCK LETTERS

Title				
Surname/family name				
First names				
Maiden name/former names				
Sex (tick box)	*Male*		*Female*	
Height				
Date of Birth				
Place of Birth	*Town*			
	County			
Your Current Home Address (to which we will reply)				
	PostCode			
A telephone number will be helpful in case you need to be contacted.	*Tel. No.*			

SECTION 2 Proof of Identity

*Your application must be accompanied by **TWO** official documents that between them clearly show your name, date of birth, current address and evidence of your physical appearance, to confirm your identity, and to enable the retrieval of the appropriate data.*

One document must be a copy or original of a photo identification document of yourself. This can be a driving license, passport, armed forces identity card or other approved document.

The second document must confirm the address of the applicant. A utility bill or tenancy agreement will be sufficient. It must show the same name as the photo identification document.

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

SECTION 3 Supply of Information

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

(a)	*View the information and receive a permanent copy*	YES / NO
(b)	*Only view the information*	YES / NO

SECTION 4 Declaration

***DECLARATION** (to be signed by the applicant)*

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

Signed by	*Date*

Warning – a person who impersonates or attempts to impersonate another may be liable to prosecution.

SECTION 5 To Help us Find the Information

You must provide us with specific details of the location and date/time of the footage you wish to request. We will not be to search the database for you. Requests will be denied if you do not provide sufficient detail to enable the relevant able footage of yourself to be found.

Date and Time of Incident	
Place Incident Happened	
Brief Details of Incident	

*Some incidents may relate to a serious, or criminal offence. The police **must** be informed of such incidents before a subject access request is made. Subject Access Requests may be denied if the request relates to a relevant incident that has not yet been alerted to the police.*

Victims of crime are strongly advised to inform the police of any potential CCTV evidence that they believe may or may not exist.

Footage is stored for 31 days. If you believe the footage you are requesting is likely to fall outside this date by the time your request has been processed, follow the below procedure:

- *Fill in the appropriate forms as normal and apply promptly*
- *Contact the System Operator by telephone on 01904 551 426*
- *Inform the System Operator that you are sending in a Subject Access Request, but believe the footage may have expired by the time it will be processed.*
- *Give the System Operator the times and dates you wish to be temporarily archived to ensure the footage is retained.*
- *Where possible, this footage will then be retained for longer than 31 days for the purpose of reviewing the Subject Access Request.*

Before returning this form	• *Have you completed ALL Sections in this form?*
Please check:	• *Have you enclosed TWO identification documents?*
	• *Have you signed and dated the form?*
	• *Have you enclosed the £10.00 (ten pound) fee?*

Further Information:

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

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

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

OFFICIAL USE ONLY

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

Application checked and legible?		***Date Application Received***	
Identification documents checked?		*Fee Paid?*	
Details of 2 Documents (see page 3)		*Method of Payment*	
		Documents Returned?	

Member of Staff completing this Section:

Name		*Location*	
Signature		*Date*	

Appendix C

Pre-approval list for access to CCTV Monitoring Rooms

Persons	Reason For Approval
CoYC employed Operators	Operation of The System
Police Inspector and above, and any Police Officer authorised by a person of that rank	Accountability
Any member of the Lay Visitor Scheme	Audit / Assessment
North Yorkshire Police CCTV Liaison Officer	Liaison
North Yorkshire Police Traffic Management Liaison Officer	Liaison
Maintenance Contractors appointed to maintain equipment within the monitoring room	Maintenance
North Yorkshire Police Premises Officer	Fabric Maintenance of the room
Assistant Director of City Strategy – Development and Transport	System Owners Representative
Police Officers with pre-booked appointments for collection of recorded material	Collection of Recorded Material
Police Officers with pre-booked appointments for review of recorded material	Review of Recorded Material

Appendix D

City of York CCTV System
Visitors Declaration of Confidentiality

I, …….....,

have been granted temporary access to part or whole of the CCTV system and monitoring room.

I hereby declare that:

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

In appending my signature to this declaration, I agree to maintain confidentiality in respect of all information gained during the course of my duties, whether received verbally, in writing or any other media format – now or in the future.

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

Signed: …..... Print Name: .....…….

Witness: ……..... Position: .....……

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

Appendix E

City of York CCTV System
Operators Declaration of Confidentiality

I, ……....., am retained by the City of York to perform the duty of CCTV Control Room Operator/have as part of my normal duties from time to time to use the CCTV equipment provided as part of The City of York CCTV system (delete whichever is not appropriate)

I have received a copy of the Code of Practice in respect of the operation and management of that CCTV System.

I hereby declare that:

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

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

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

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

Signed: …..... Print Name: .....…….

Witness: ……..... Position: .....……

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