

# **STOCKTON ON TEES BOROUGH COUNCIL**

## **THE SECURITY CENTRE CCTV MONITORING SCHEME**

### **CODE OF PRACTICE FOR CCTV SCHEME (BS7958 and BS7858)**

<b>Author</b>	Marc Stephenson
<b>Position</b>	Operations Manager
<b>Date of Last Amendment</b>	6 <sup>th</sup> December 2017
<b>Date of Next Review</b>	1 <sup>st</sup> April 2018

## CONTENTS

<b>1.0</b>	<b>INTRODUCTION AND DEFINITIONS</b>	
<b>1.2</b>	OWNERSHIP	
<b>1.3</b>	CCTV MISSION STATEMENT	
<b>1.4</b>	CODES OF PRACTICE MISSION STATEMENT	
<b>1.5</b>	DEFINITIONS	
<b>1.6</b>	SYSTEM DESCRIPTION	
<b>1.7</b>	KEY PERSONELL	

<b>2.0</b>	<b>CHANGES TO THE CODE OF PRACTICE</b>	
<b>2.1</b>	CONSULTATION	
<b>2.2</b>	SUPLEMENTARY DOCUMENTATION	

<b>3.0</b>	<b>OBJECTIVES OF THE CCTV SCHEME AND CODE OF PRACTICE</b>	
<b>3.2</b>	OBJECTIVES OF THE SCHEME	

<b>4.0</b>	<b>FUNDAMENTAL PRINCIPLES AND POLICIES</b>	
<b>4.1</b>	RIGHTS OF PRIVACY	
<b>4.2</b>	PRINCIPLES OF MANAGEMENT OF THE SCHEME	
<b>4.3</b>	POLICY OF THE SCHEME AND SIGNAGE	
<b>4.4</b>	POINT OF CONTACT	
<b>4.5</b>	RELEASE OF INFORMATION TO PUBLIC	
<b>4.6</b>	RELEASE OF INFORMATION TO STATUTORY BODIES	
<b>4.7</b>	ANNUAL POLICY REVIEW	

<b>5.0</b>	<b>DATA PROTECTION AND LEGISLATION</b>	
<b>5.1</b>	DATA PROTECTION REGISTRATION	
<b>5.2</b>	HUMAN RIGHTS ACT 1998	
<b>5.3</b>	CRIMINAL PROCEDURES AND INVESTIGATIONS ACT 1996	
<b>5.4</b>	FREEDOM OF INFORMATION ACT 2000	
<b>5.5</b>	REGULATION OF INVESTIGATORY POWERS ACT 2000	
<b>5.6</b>	SURVEILLANCE CAMERA CODE OF PRACTICE	
<b>5.7</b>	CRIME & COURTS ACT 2013	

<b>6.0</b>	<b>ACCOUNTABILITY</b>	
<b>6.1</b>	SUPPORT OF PRINCIPLES	
<b>6.2</b>	RESPONSIBILITIES	
<b>6.3</b>	ACCOUNTABILITY	
<b>6.4</b>	ANNUAL ASSESSMENTS	
<b>6.5</b>	AUDITS	

<b>6.6</b>	COMPLAINTS	
<b>6.7</b>	PERSONNEL	

<b>7.0</b>	<b>CONTROL ROOM MANAGEMENT AND OPERATION</b>	
<b>7.1</b>	GENERAL	
<b>7.2</b>	RESPONSE TO INCIDENTS	
<b>7.3</b>	MAKING RESPONSE AND TIME SCALES	
<b>7.4</b>	OBSERVATION AND RECORDING INCIDENTS	
<b>7.5</b>	SUCCESSFUL RESPONSE	
<b>7.6</b>	OPERATION OF THE SYSTEM BY POLICE	

<b>8.0</b>	<b>PRIVACY AND DISCLOSURE ISSUES</b>	
<b>8.1</b>	PRIVACY	
<b>8.2</b>	DISCLOSURE POLICY	
<b>8.3</b>	ACCESS TO RECORDED IMAGES	
<b>8.4</b>	VIEWING OF RECORDED IMAGES	
<b>8.5</b>	OPERATORS AWARENESS	
<b>8.6</b>	REMOVAL OF MEDIUM FOR VIEWING	
<b>8.7</b>	ACCESS TO DATA BY THIRD PARTIES	
<b>8.8</b>	DISCLOSURE IN THE PUBLIC INTEREST	
<b>8.9</b>	DATA SUBJECT ACCESS	
<b>8.10</b>	PROVISION OF DATA TO INDIVIDUALS	
<b>8.11</b>	OTHER RIGHTS	
<b>8.12</b>	MEDIA DISCLOSURE	

<b>9.0</b>	<b>RECORDED MATERIAL MANAGEMENT</b>	
<b>9.1</b>	GENERAL	
<b>9.2</b>	QUALITY AND MAINTENANCE	
<b>9.3</b>	DIGITAL RECORDING	
<b>9.4</b>	MAKING RECORDINGS	
<b>9.5</b>	PRINTS	

<b>10.0</b>	<b>DOCUMENTATION</b>	
<b>10.1</b>	GENERAL	
<b>10.2</b>	LOGS	
<b>10.3</b>	ADMINISTRATIVE DOCUMENTS	

<b>Appendix A</b>	AGREEMENT BETWEEN STOCKTON BOROUGH COUNCIL AND CLEVELAND POLICE	
<b>Appendix B</b>	LOCATION OF CCTV SIGNS IN STOCKTON ON TEES.	

## **1.0 INTRODUCTIONS & DEFINITIONS**

### **1.1 Introduction**

This Code of Practice shall apply to the closed circuit television surveillance schemes known as the Stockton Borough Council CCTV network, or hereinafter “the scheme”. The scheme initially comprises of cameras located in specific external and internal locations within the Stockton on Tees area, with control, monitoring and recording facilities at a dedicated location. A problem orientated process was utilised to assess the appropriateness of CCTV in the Stockton on Tees area, with full consideration given on the impact to the privacy of residents. The cameras have therefore been sited to capture images which are relevant to the purposes for which the scheme has been established.

The scheme also benefits from Home Office approval to monitor a number of bus lane cameras within the area. All of the cameras within the scheme are fully operational with pan, tilt and zoom capability.

For the purpose of the Data Protection Act, the ‘data controller’ is Stockton on Tees Borough Council. The scheme has been notified to the Information Surveillance Commissioner as required by the Data Protection Act 1998.

Details of key personnel and points of contact regarding the scheme are shown in this document at 1.7 of this document.

### **1.2 Ownership**

The scheme is owned by Stockton on Tees Borough Council who is responsible for the management, administration and security of the system. Stockton on Tees Borough Council will ensure the protection of individuals and the public by complying with the Codes of Practice.

### **1.3 Closed Circuit Television Mission Statement**

The system is a vital tool in contributing to the Councils vision for a safer environment for both the communities our residents live in, but also for visitors to our town centres, parks and open spaces. We will have neighbourhoods in which our residents feel safe, proud and have sense of belonging and ownership. We do this by supporting the aims and objectives of the Safer Stockton Partnership, in line with the Community Safety Plan, but by also developing innovating working methods in order to deliver an efficient and lean operating model which is fit for purpose and will meet future demand.

### **1.4 Codes of Practice Mission Statement**

To inspire public confidence by ensuring that all public area Closed Circuit Television (CCTV) systems which are linked to the CCTV Control and Monitoring Room (The Security Centre)

are operated in a manner that will secure their consistent effectiveness and preserve the civil liberty of law abiding citizens at all times.

## 1.5 Definitions

- 1.5.1 **The CCTV control and monitoring room** shall mean the secure area of a building where CCTV is monitored and where data is retrieved, analysed and processed. It is also the location where calls may be received from various Council services on an out of hours basis.
- 1.5.2 **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.
- 1.5.3 **The retrieval system** means the capability, in any medium, of effectively capturing data that can be retrieved, viewed or processed.
- 1.5.4 **CCTV system** means the surveillance items comprising cameras and associated equipment for monitoring, transmission and controlling purposes, for use in a defined zone.
- 1.5.5 **The distributed system** means any subsystem, any part of which may be linked temporarily or permanently for remote monitoring within the CCTV system.
- 1.5.6 **Data** shall mean all information, including that about a person in the form of pictures, and any other associated linked or processed information.
- 1.5.7 **Personal Data** means data which relates to a living individual who can be identified:
- a) from that data or;
  - b) from that data and other information which is in the possession of or is likely to come into the possession of, the data controller.
- 1.5.8 **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.
- 1.5.9 **An incident** is an activity that raises cause for concern that the safety or security of an individual or property including vehicles that may be compromised or that an offence has been, is being or is about to be, committed, or that an occurrence has taken place warranting specific action by an operator.
- 1.5.10 **The owner** is Stockton Borough Council, the organisation with overall responsibility for the formulation and implementation of policies, purposes and control of the scheme.

- 1.5.11 **The manager** (Stockton Borough Council) 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.
- 1.5.12 **Data controller** means a 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.
- 1.5.13 **Contractor** is a party contracted by the owner to undertake the day to day operation of their CCTV system, either utilising the owner's facilities or supplying a full monitoring service.
- 1.5.14 **Operators** are employees of the Data Processor and are specifically designated to carry out the physical operation of controlling the CCTV system and the data generated. All operators are screened, trained and licensed to the standards required in the Private security Industry Act 2001.
- 1.5.15 **Recording material** means any medium that has the capacity to store data and from which data can later be recalled irrespective of time.
- 1.5.16 A **hard copy print** is a paper copy of a live image or images, which already exist on recorded material.

## 1.6 System description

- 1.6.1 The Closed Circuit Television system referred to in this document has been introduced into Stockton on Tees Borough Council areas. The schemes are owned by Stockton on Tees Borough Council and operated by specifically employed internal staff.
- 1.6.2 The owner, contractor, operators and all partners will work in accordance with the Codes. The partners will have no involvement in the operating of the system with the exception of the Police and authorised and trained personnel.
- 1.6.2 This Code of Practice shall apply to the closed circuit television surveillance systems known as the Stockton on Tees Borough Council CCTV network.
- 1.6.3 The system consists of static and fully functional (pan, tilt and zoom) cameras which sends pictures to the Stockton Borough Council control, monitoring and recording facility via a wireless network.
- 1.6.4 Images from all cameras are monitored and recorded simultaneously throughout a 24 hour period 365 days each year.
- 1.6.5 There is also a dedicated CCTV transmission link to Police control rooms operating within the areas of CCTV coverage where live pictures and events can be monitored.

- 1.6.6 A current deployment of 149 high quality cameras both fully functional with pan, tilt and zoom and static are in use across the Stockton on Tees area.
- 1.6.7 The physical and intellectual rights in relation to any and all material recorded within the Stockton Borough Council Control and Monitoring facility shall at all times remain in the ownership of Stockton on Tees Borough Council.

## **1.7 Key Personnel**

1.7.1 The key Council personnel involved in the day to day running of the CCTV network, or The Scheme, are as follows;

- Community Services Manager – Craig Willows
- Cleansing, Waste and Security Services Manager – Marc Stephenson
- CCTV Supervisor – Paul Leonard

## **2.0 CHANGES TO THE CODE OF PRACTICE**

2.1 Any major changes to this Code of Practice (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 will, and upon the arrangement of all organisations with a participatory role in the operation of the system.

2.1.1 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.

## **3.0 OBJECTIVES OF THE CCTV SCHEME & CODE OF PRACTICE**

3.1 This Code of Practice is to detail the management, administration and operation of the closed circuit television (CCTV) network in the Stockton Borough Council area and the associated Control and Monitoring Facility.

3.1.1 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.

3.1.2 The owners, CCTV Operators and users of the CCTV systems and associated safety and security equipment connected to the Control, Monitoring and Recording facility 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.

3.1.4 The owners, CCTV Operators, users and any visitors to the Control, monitoring and recording facility 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.

## 3.2 Objectives of the scheme

3.2.1 The objectives of The Scheme as determined by the partnership which form the lawful basis for the processing of data area:

- (a) To reduce crime and the fear of in the Borough
- (b) Reducing disorder and anti-social behaviour and the fear of it in the Borough
- (c) To reduce the fear of crime in the Borough
- (d) To protect Council assets and property
- (e) To protect private businesses and public assets and property
- (f) Reduce vehicle crime both on street and in public car parking within the Borough
- (g) Positively impact on environmental factors such as littering, vandalism, dog fouling and fly tipping
- (h) providing assistance and reassurance to the public in emergency situations
- (i) Assist with traffic management, bus lane enforcement and crowd control during public and private events
- (j) To check infringements of the Market Charter and associated regulations
- (k) To assist in supporting civil proceedings which will help detect crime

## 4.0 FUNDAMENTAL PRINCIPLES & POLICIES

### 4.1 Rights of Privacy

4.1.1 Stockton 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.

4.1.2 Cameras will not be used to look into private residential properties. Where the surveillance equipment permits it, then 'privacy zones' will be programmed into the system, as required, in order to ensure that the cameras do not survey areas which the public have a reasonable belief of privacy. If such zones cannot be programmed in to the system, operators will receive specific guidance and instruction regarding the use of the equipment in these areas.

4.1.3 Clear signs are displayed on entrance roads as well as key points around the area. The purpose of these signs are to inform members of the public that surveillance is being undertaken and they also serve to outline the purpose of such activity, providing a single point of contact for any questions, concerns or queries. Information on the location of these signs can be found at Appendix B.

4.1.4 The single point of contact for all correspondence is; The Security and Surveillance Manager, The Security Centre, The Square, Stockton on Tees, TS18 1TE. 01642 528989, [security.surveillance@stockton.gov.uk](mailto:security.surveillance@stockton.gov.uk).

### 4.2 Principles of management of the scheme



- 4.2.1 Prior to the installation of 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.
- 4.2.2 Cameras will be sited to ensure that they can produce images of the right quality, taking into account technical and environmental issues.
- 4.2.3 If wireless transmission systems are used to control CCTV equipment, sufficient safeguards will be in place to protect them from being intercepted.
- 4.2.4 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 this Code of Practice.
- 4.2.5 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.
- 4.2.6 The scheme will be operated with due regard for the privacy of the individual.
- 4.2.7 The public interest in the operation of the scheme will be recognised by ensuring the security and integrity of operational procedures.
- 4.2.8 The system will only be operated by staff who are Security Industry Authority trained and licensed.

## **5.0 DATA PROTECTION ACT AND OTHER LEGISLATION**

### **5.1 Data Protection Registration**

- 5.1.1 The scheme is registered with the Data Protection Commissioner. Registration Number Z590889X. The scheme will be managed in accordance with the principles of the Data Protection Act 1998.
- 5.1.2 Stockton Borough Council has a policy of not allowing footage captured by the system, to be sold to media companies.
- 5.1.3 The 'data controller' for The Scheme is Stockton on Tees Borough Council and day-to-day responsibility for the data will be devolved to The Scheme Manager, Marc Stephenson.
- 5.1.4 All data will be processed in accordance with the principles of the Data Protection Act 1998, which includes, but not limited to;

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

## **5.2 Human Rights Act 1998**

5.2.1 The system will be operated by or on behalf of a public authority, the authority has considered the wider human rights issues and in particular the implications of the European Convention on Human Rights, Article 8 (the right to respect for private and family life).

- Everyone has the right to respect for his private and family life, his home and his correspondence.
- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
- Therefore, to comply with Article 8 (1), and Article 8 (2) Stockton Borough Council will always considers the following:

Proportionality - Article 4.2.1, 4.2.2, 4.2.3 and 4.2.6 of the code of practice

Legality - Article 4.2.7 and 4.2.8 of the code of practice

Accountability - Article 4.2.10 and 4.2.11 of the code of practice

Necessity/Compulsion - Article 4.2.3 of the code of practice

Any infringement by a public authority of another's rights must be justified. If this is not the case then it will not be appropriate to use CCTV.

## **5.3 Criminal Procedures and Investigations Act 1996**

5.3.1 The Criminal Procedures and Investigations Act 1996 came into effect in April 1997 and introduced a statutory framework for the disclosure to defendants of material which the prosecution would not intend to use in the

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).

#### **5.4 Freedom of Information Act 2000**

- 5.4.1 If a request for images is received via a FOI 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.
- 5.4.2 Any other requests not involving identification of individuals can be disclosed but only if it does not breach the data protection principles.

#### **5.5 Regulation of Investigatory Powers Act 2000**

- 5.5.1 The Regulation of Investigatory Powers Act (RIPA) 2000 came into force on 2<sup>nd</sup> October 2000. It places a requirement on public authorities listed in Schedule 1: Part 1 of the act to authorise certain types of covert surveillance during planned investigations. The Scheme Manager recognises the implications of the Regulation of Investigatory Powers Act 2000 and manages the system to comply with the latest guidance and statutory procedure.
- 5.5.2 Any use of this system for directed surveillance which is considered to fall within the scope and meaning of RIPA will be subject to authorisation by the relevantly named person. Any request for such a use from Cleveland Police or other Police Authorities or law Enforcement Agencies requires written confirmation from an officer of the rank of inspector (equivalent person in requesting organisation) or above. A copy of the RIPA must be provided. This will be registered with the authorities' central register and held within the authorities' legal sector.
- 5.5.3 Directed surveillance is defined in subsection (2) as covert surveillance that is undertaken in relation to a specific investigation or a specific operation, which is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance. If a control room operator is carrying out normal everyday observations by operating a particular camera to gain the best information (albeit it may not be the most obvious camera to use) or the nearest to the incident being observed, that use will not be deemed to be "covert" under the terms of the act. It is using modern technology to the advantage of the operator. It will only be where CCTV cameras are to be used in a planned, targeted way to gain private information that the requirements of authorised directed surveillance need to be met.
- 5.5.4 If requested to operate cameras as part of a planned operation where the subject is: unaware that targeted surveillance is, or may be, taking place and private information is to be gained, and it involves systematic surveillance of an individual/s (whether or not the target of the operation) a RIPA "directed surveillance" authority must be obtained. It must

indicate specific reasons and be necessary for the purpose of preventing or detecting crime or of preventing disorder.

- 5.5.5 Directed Surveillance is defined as covert surveillance that is undertaken in relation to a specific investigation or a specific operation which is likely to result in the obtaining of private information about a person (whether or not specifically identified for the purposes of the investigation) or operation. And otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this part to be sought for the carrying out of the surveillance. Covert Surveillance is covert if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place. All Direct and covert surveillance can only go ahead with authorised RIPA paper work signed by an authorised officer.
- 5.5.6 Under normal circumstances town centre CCTV Systems and the Code of Practice are not covered by the RIPA. However, if operators are tasked to assist in a pre-planned operation then a 'directed surveillance' authority may be required.
- 5.5.7 Every RIPA authority must be properly thought through and that 'thought process' clearly demonstrated and recorded on the application. Whenever an authority is issued it must be regularly reviewed as the investigation progresses and it must be cancelled properly upon conclusion. The completion of these stages will be looked at during any inspection process. In cases where there is doubt as to whether an authorisation is required or not, it may be prudent to obtain the necessary authority verbally and then later in writing using the forms. Forms are available from the local Authority Legal Sector. To maintain confidentiality, it is possible for the Police not to release full details of the request, other than sufficient information to carry out the surveillance. Detailed procedure can be found in Stockton Borough Councils Corporate Policy and Procedures document on the regulation of Investigatory Powers Act 2000.

## **5.6 Surveillance Camera Code of Practice**

- 5.6.1 The Code of Practice was a requirement of the Protection of Freedoms Act 2012 and sets out guidelines for CCTV and Automatic Number Plate Recognition (ANPR) systems to ensure their use is open and proportionate and that they are able to capture quality images that give police a better chance to catch criminals and cut crime.
- 5.6.2 The code has been built upon 12 guiding principles, which provide a framework of good practice that includes existing legal obligations. Those existing obligations include the processing of personal data under the Data Protection Act 1998, a public authority's duty to adhere to the Human Rights Act 1998 and safeguards under the Regulation of Investigatory Powers Act 2000 associated with the use of directed and covert surveillance by a public authority. The use of a surveillance camera system must:
1. Always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need
  2. Take into account its effect on individuals and their privacy

3. Have as much transparency as possible, including a published contact point for access to information and complaints
4. Have clear responsibility and accountability for all surveillance activities including images and information collected, held and used
5. Have clear rules, policies and procedures in place and these must be communicated to all who need to comply with them
6. Have no more images and information stored than that which is strictly required
7. Restrict access to retained images and information with clear rules on who can gain access
8. Consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards
9. Be subject to appropriate security measures to safeguard against unauthorised access and use
10. Have effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with
11. Be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value, when used in pursuit of a legitimate aim
12. Be accurate and kept up to date when any information is used to support a surveillance camera system which compares against a reference database for matching purposes.

5.6.3 Whilst the above principles are voluntary, Local Authorities must have regard to them and Stockton on Tees Borough Council will work to achieve continued compliance with the requirements.

## **6.0 ACCOUNTABILITY**

### **6.1 Support of Principles**

- 6.1.2 The Councils Cabinet Member for Housing and Community Safety will consider any necessary report, on the operation of The Scheme. All such reports will also be presented to the Safe Stockton Partnership, which is the statutory local Community Safety Partnership for the Borough which carried out the duties created by sections 5 and section 6 of the Crime and Disorder Act 1998.
- 6.1.3 The manager/supervisor shall be accountable to the owner of the scheme and will provide periodic progress reports on the scheme. The manager/supervisor will resolve technical and operational matters.
- 6.1.4 Failure of the operators to comply with the procedures and code of practice should be dealt with by the manager/supervisor. Person(s) misusing the system will be subject to

disciplinary or legal proceedings in accordance with the Stockton on Tees Borough Council Disciplinary Policy.

- 6.1.4 Copies of this Code of Practice are available to members of the public online ([www.stockton.gov.uk](http://www.stockton.gov.uk)) or upon request to the Security and Surveillance Manager.

## **6.2 Hierarchy of Responsibilities**

### **6.2.1 The Owner**

The owner shall be responsible for policy, effective management and public relations of the scheme. They shall produce a written policy and be responsible for its implementation. This shall be carried out in consultation with users of the scheme and provide for the release of information relating to the operation of the system. The owner is responsible for dealing with complaints, and ensuring a fair system of staff selection and recruitment is adopted for staff employed in the control and monitoring environment. The role of owner also includes all statutory responsibilities including the role of “data controller” as prescribed by the Data Protection Act 1998 Section 1 Subsection 1(1).

### **6.2.2 The Manager**

The manager or designated member of staff should undertake regular reviews of the documented 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 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
- Liaison with police and other agencies
- Maintenance of the quality of recording and monitoring equipment

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 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 and Procedural Manual. Dealing with breaches of the codes and disciplinary measures shall lie with the manager.

### 6.2.3 **The Supervisor and Team Leaders**

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 confidentially. In the Managers absence the Supervisor will have responsibility for:

- Release of data to third parties who have 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 media
- Liaison with police and other agencies

The supervisor 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.

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

### 6.2.4 **The Operators**

The operators will be responsible for complying with the code of practice and procedural manual. 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 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 CCTV maintenance contractor immediately any equipment defect that may occur.

### 6.2.5 **Contractor's Responsibilities**

There are a number of contractors responsible for;

- 1) Maintenance of CCTV equipment
- 2) Maintenance of door entry systems

The response provided by contractors is the subject of a written contract and records of responses are maintained

## 6.4 **Annual Assessment**

6.4.1 An annual assessment of the scheme will be undertaken by an independent appointed person to evaluate the effectiveness of the system. This will include annual reviews of the

scheme's operation, performance and working practices and, where appropriate make recommendations for improvements. The results will be assessed against the stated purposes of the scheme. If the scheme is not achieving its purpose modification and other options will be considered.

6.4.2 The results of the assessment will be made available through the Stockton Borough Council website or upon written request to the network Manager.

6.4.3 The Information Commissioner's CCTV Code of Practice stipulates that the system should be reviewed annually to determine whether CCTV continues to be justified. It further states that it is necessary to establish the system's effectiveness to ensure that it is still doing what it was intended to do. If it does not achieve its purpose, it should be stopped or modified.

## **6.6 Complaints**

6.6.1 A member of the public wishing to make a complaint about the system may do so through Stockton Borough Council complaint procedure.

6.6.2 A report on the numbers of complaints will be collated by the systems manager or designated member of staff in order to assess public reaction to, and opinion of, the use of the system. The annual report will contain details of the numbers of complaints received, the time taken to acknowledge and respond to complaints, the method of receiving and handling complaints and the degree of satisfaction in handling complaints.

## **6.7 Personnel**

### **6.7.1 Security screening**

All personnel employed to control/operate or manage the scheme will be security screened in accordance with British Standard 7858: *Code of practice for screening of personnel in a security environment*. In addition, they will also be subject to vetting to none police staff anti-terrorist security screening standards.

### **6.7.2 Training**

All operators are or will be trained to the criteria required by the private Security Industry Act 2001 and licensed by the Security Industry Authority for Public Space Surveillance systems

All persons employed to act as operators of the system are trained to the highest available industry standard. Training has been completed by suitably qualified persons and has included:

- Terms of employment
- The use of all appropriate equipment
- The operation of the systems in place
- The management of recorded material including requirements for handling and storage of material needed for evidential purposes.
- All relevant legal issues including Data Protection and Human Rights



- Progression to nationally recognised qualifications
- Recognise and understanding privacy and disclosure issues
- The disciplinary policy

#### 6.7.2 Contractor's

There are special condition's imposed upon contractor's carrying out works on the system. It should be noted that wherever possible CCTV installation and maintenance contractors should not have sight of any recorded data.

## 7.0 CONTROL ROOM MANAGEMENT AND OPERATION

### 7.1 Access to Control Room

7.1.1 Access to the monitoring area will be strictly controlled. Security of the Control Room shall be maintained at all times.

7.1.2 Only those persons with a legitimate purpose will be permitted access to the control and monitoring Room.

7.1.3 The Supervisor or in his/her absence the Deputy, is authorised to determine who has access to the monitoring area. This will normally be:

- Operating staff
- The Manager/Supervisor
- Police officers requiring to view images of a particular incident, or collecting/returning images being considered for intelligence or evidential purposes. These visits will take place by prior appointment
- Engineers and cleaning staff
- Independent Inspectors appointed under this Code of Practice may visit the control room without prior appointment.
- Organised visits by authorised persons in controlled circumstances

7.1.3 For reasons of security and confidentiality, access to the CCTV monitoring room is restricted in accordance with this Code of Practice. However, in the interest of openness and accountability, anyone wishing to visit the room may be permitted to do so, subject to the approval of, and after making prior arrangements with, the manager of the System. All visitors to the monitoring area, including Police Officers, will be required to sign a visitors log and a declaration of confidentiality.

7.1.4 All monitors which are part of the scheme are contained within a secure Control Room designed and built to the British Standard *BS5979 Part 2*, with access controlled by:

- Steel perimeter fence
- Internal CCTV in all internal and external public spaces
- Electronically operated security doors to the building
- 'Airlock' system to enter the Control Room itself
- The Control Room is not left unattended.

## **7.2 Response to an incident**

- 7.2.1 A record of all incidents will be maintained in the incident log. Information will include anything of note that may be useful for investigative or evidential purposes.

## **7.3 Who makes the response and the time scale**

- 7.3.1 Incidents of a criminal nature will be reported to Cleveland Police. The response will be made by the Police Service in accordance with their policies. All other incidents will be reported to the relevant authority for the appropriate action to be undertaken in accordance with individual policy and procedures.

## **7.4 Observation and recording of incidents**

- 7.4.1 Recording will be throughout the 24 hour period in time lapse mode. Wherever possible the system will be monitored 24 hours a day. In the event of an incident being identified there will be particular concentration on the scene.

## **7.6 Operation of the System by the Police**

- 7.6.1 There is a monitor facility installed at specific Police Stations, namely Ladgate Lane Police Headquarters. Under certain circumstances the Police may make a request to view a number of cameras to which this Code of Practice applies. Following agreement by the control room supervisor at the time, the Police communications supervisor will provide sufficient information to the operator of the genuine need for such surveillance.
- 7.6.2 In the event of the police requesting use of the equipment from within the CCTV control room to monitor situations, the monitoring room will continue to be staffed and equipment operated by, only those personnel who are authorised to do so and who fall within the terms of this Code.
- 7.6.3 In very extreme circumstances such as a major incident 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. A request for total exclusive control must be made in writing by a Police Officer not below the rank of Chief Superintendent (or designated deputy).
- 7.6.4 Once the police undertake any of the above they become responsible under the Data Protection Act 1998.
- 7.6.5 A telephone and radio link through to the police station is available to effectively relay information on incidents that arise.

## **8.0 PRIVACY AND DISCLOSURES ISSUES**

### **8.1 Privacy**

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

## **8.2 Disclosure Policy**

8.2.1 The following principles must be adhered to:

- a) 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.
- b) 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.
- c) The Data controller will only disclose to third parties who intend processing the data for purposes which are deemed compatible with the objectives of the CCTV scheme.
- d) 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.
- e) Recorded material will only be used for the purposes defined in the objectives and policy.
- f) Access to recorded material will be in accordance with policy and procedures.
- g) Information will not be disclosed for commercial purposes and entertainment purposes.
- h) All access to the medium on which the images are recorded will be Documented.
- i) 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.
- j) Viewing of the recorded images should take place in a restricted area.

## **8.3 Access to recorded images**

8.3.1 Access to recorded images will be restricted to the manager or designated member of staff who will decide whether to allow requests for access by third parties in accordance with the disclosure policy.

8.3.2 Police may apply for access in accordance with an agreement with the owner where the Police reasonably believe access to specific footage is necessary for the investigation and detection of a particular offence or offences or for the prevention of crime. Police may obtain access under the provisions of the Police and Criminal Evidence Act 1984 (PACE)

8.3.3 Material provided to the Police shall at no time be used for anything other than the purpose specified and identified when the tape is released to the Police by the control room. Arrangements may be made from time to time for a police officer appointed in accordance

with liaison arrangements to visit the control room and confirm that agreed procedures are being followed.

8.3.4 Access to material may be obtained in connection with civil disputes by court order or be extended to lawyers acting for defendants or victims in connection with criminal proceedings.

8.3.5 No other access will be allowed unless approved by the individual appointed to have day-to-day responsibility for the scheme for reasons, which fall within the purposes and objectives of the scheme and in accordance with the Code of Practice.

#### **8.4 Operators**

8.4.1 All operators are trained in their responsibilities in relation to access to privacy and disclosure issues.

#### **8.7 Access to data by third parties**

8.7.1 Access to images by third parties will only be allowed in limited and prescribed circumstances. In these cases, disclosure will be limited to the following:-

- law enforcement agencies where the images recorded would assist in a specific criminal enquiry
- prosecution agencies
- legal representatives
- The people whose images have been recorded and retained (Data Subject) unless disclosure to an individual would prejudice the criminal enquiries or criminal proceedings.
- Where the relevant legislation allows access.
- Public bodies that wish to pursue civil or criminal cases

8.7.2 All requests for access or for disclosure will be recorded. If access or disclosure is denied, the reason should be documented.

8.7.3 If access to or disclosure of the images is allowed, details will be documented.

8.7.4 Recorded images should 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.

8.7.5 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 and the reason documented.

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

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

#### **8.7 Data subject access disclosure**

- 8.8.1 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 individual's rights under this section of the Code of Practice.
- 8.8.2 Data subjects requesting access will be provided with a standard subject access request form and accompanied leaflet describing the types of images recorded and retained and the purposes for recording and retention.
- 8.8.3 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;
  - b) The person gives sufficient and accurate information about a time and place;
  - c) Information required as to the identification of the person making the request;
  - a) The Data Controller only shows information relevant to the search.
- 8.8.4 If a copy of the footage is requested, 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.
- 8.8.4 If on the other hand images have been obtain 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 or assessing how an employee is performing. These activities will still be covered by the DPA and reference should be made to Section 8.2.2 of these Codes of Practice prior to the release of such data.
- 8.8.5 Only data pertaining to that person is copied unless consent from all third parties is received. 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
- 8.8.6 All subject access requests should be dealt with by the manager or designated member of staff operating within the corporate team designated to deal with such requests in the first instance.
- 8.8.7 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.
- 8.8.8 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.
- 8.10 Provision of data to the individual**

- 8.10.1 The owner/manager 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 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.
- 8.10.2 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

## **9.0 RECORDED MATERIAL MANAGEMENT**

### **9.1 Retention of Images**

- 9.1.1 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.
- 9.1.2 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 along the evidence chain.
- 9.1.3 Security measures will be taken to prevent unauthorised access to, alteration, disclosure, destruction, accidental loss or destruction of recorded material.
- 9.1.4 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.
- 9.1.5 Images retained for evidential purposes will be retained in a secure place where access is controlled.

### **9.2 Quality and Maintenance**

- 9.2.1 In order to ensure that clear images are recorded at all times the equipment for making recordings and the associated security equipment will be maintained in good working order with regular servicing in accordance with the manufacturer's instructions. In the event of a malfunction the equipment will be repaired within specific time scales which will be scheduled within the maintenance agreement. All documentation relating to the equipment and its servicing and malfunction is retained in the control room and will be available for inspection and audit.

### **9.3 Digital Recordings**

9.3.1 In a digital CCTV system, the register should show the life of the media at all stages whilst in the owner's possession. Such a register may also show itself to be useful in enabling evaluation of the CCTV scheme.

The register should include the following:

- Unique equipment reference number(s);
- Details of purchase (i.e., from whom purchased and delivery date);
- Time/date/person removing equipment from secure storage for use;
- Time/date/person returning equipment to secure storage after use;
- Remarks column to cover additional points (e.g., erase/destroy/handed over to law enforcement agencies/removed from recording machine);
- Time and date of delivery to the law enforcement agencies, identifying the law enforcement agency officer concerned;
- In the event of a non-automated system of erasure of data, the time / date / person responsible for erasure and/or destruction.

## **9.5 Photographs**

9.5.1 Photographs will only be made when absolutely necessary. All photographs will remain the property of the scheme owner. The taking of photographs will be recorded in a register to be retained in the control room (as detailed in 9.3).

**Code of Practice in Respect of the  
Operation of Stockton on Tees Borough Council CCTV Network**

***Agreed by***  
**Stockton on Tees Borough Council**  
**And**  
**Cleveland Police**

***Certificate of Agreement***

*The content of both this Code of Practice are hereby approved in respect of the Stockton on Tees Borough Council 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** Stockton on Tees Borough Council -

Signature:

Name:

Position held:

Dated:

**Signed for and on behalf of** Cleveland Police -

Signature:

Name:

Position held:

Dated:



## Location of advanced signage

Area of Installation	Point of Reference	Date Installed
Norton Village, Leven Road	Lampost Opposite The Village Shop (19L2360)	23.5.16
Norton Village, High St Entrance	Lampost near Blackwell Butchers	15.6.16
Norton Village, High St Entrance	Lampost near Red Lion Public House	15.6.16
Norton Village, High St Entrance	Lampost opposite the Methodist Church (Norton Road)	15.6.16
Oxbridge Lane, Stockton	Lampost opposite the Allotment Gardens	15.6.16
Bowesfield Lane, Stockton	Lampost opposite the PM Cook Accountants (15B330)	23.5.16
Durham Road, Stockton	Lampost opposite St John's Church (No number)	23.5.16
Durham Road Bypass, Stockton	Lampost on the entrance to the road from Durham Rd Roundabout	15.6.16
A1305 near Bridge Road Ent, Stockton	Lampost on Junction / Roundabout - No number	10.7.16
Norton Road, Stockton	Lampost opposite Victoria Business Centre (Ent to high st)	10.7.16
Norton Road, Stockton	Lampost opposite Pickerings Lifts	15.6.16
Yarm Lane, Near Richardson Road	Lampost on Junction of Yarm Road / Hartburn Lane	10.7.16
Church Road, Stockton	Lampost opposite the Roundabout Kitchen	15.6.16
Yarm High Street, Yarm	Lampost opposite the Bluebell Public House	15.6.16
Thorntree Road, Thornaby	Near shopping parade. No Lampost Number	20.4.16
Langley Avenue, Thornaby	Junction of Mansfield Av. No Lampost Number	20.4.16
Lanehouse Road, Thornaby	Junction of Oxford Road. Lampost No <b>8L2315</b>	20.4.16
Cobden Street, Thornaby	Junction of Anderson Road. Lampost No <b>4C636</b>	20.4.16
Thorntree Shops, Black Path	Front of shopping Parade. No Lampost Number	20.4.16
Briar Road, Thornaby	Junction of Maple Av. Lampost No <b>A18E1044</b>	20.4.16
High Newham Road, Hardwick	Junction of Scurfield Road.	20.4.16

	Lampost No <b>9H1812</b>	
Redhill Road, Roseworth	Opposite Shopping Parade. On the camera Column	20.4.16
Romford Road, Roseworth	Children's Play Area. Lampost No <b>14R3313</b>	20.4.16
Rochester Road, Roseworth	Children's Play Area. Lampost No <b>19R3302</b>	20.4.16
Infinity North Bridge, Stockton	Near Bridge and Thirteen office. No lampost Number.	20.4.16
Infinity South Bridge, Stockton	Near Bridge and Unversity. No lampost Number.	20.4.16
Wade Avenue, Stockton	On Green Belt. On Camera Column.	20.4.16
Cromwell Avenue, Stockton	Junction of Wade Avenue. Lampost No <b>5C717</b>	20.4.16
Raleigh Road, Norton	Junction of Waterford Road. No lampost Number	20.4.16
Balmoral Terrace, Oxbridge	Junction of Malborough Road. On Camera Column	20.4.16
Cowper Road, Tilery, Stockton	Junction of Kingston Road. On Camera Column	20.4.16
Beckfield Avenue, Ingelby Barwick	Parade of Shops. On the Camera Column	20.4.16