

COMMUNITY SAFETY CCTV – ANNUAL CCTV STANDARDS REPORT.

This document is designed to assist both Commissioning Officers and members of the general public in terms of Operational Issues of a CCTV network.

Date of Review	1 st April 2022	Responsible Officer	Paul Leonard
Contact Details of Responsible officer	01642 528989	Next Review Date	1 st April 2022
Authorising Officer	Marc Stephenson	Date Authorised	25 th May 2021
Operational Requirements			
Requirements		Review of Compliance	Further Actions Required
1	Does the system continue to meet the purpose for which it was installed?	The system continues to meet its purpose in terms of deterring, preventing and detection of crime, working to all legal requirements.	
2	Have any complaints been received about an individual camera or the whole/part of the system? If yes, what was the outcome?	No complaints have been received up until the date of this review from members of the public. We have been subject to a number of Freedom of Information Requests however this has also not resulted in further follow up.	
3	Has the location of each camera been reviewed to ensure they remain suitable?	Each camera location is reviewed on an annual basis making sure the location is suitable for the required purpose. All new installations are reviewed, and a privacy impact assessment undertaken.	
4	Is there a Comprehensive maintenance and cleaning regime in place?	A specific maintenance and cleaning contract is in place and is provided by specialist engineers who is contracted to maintain the system until October 2021.	
5	Is there appropriate and sufficient signage in places to warn people that CCTV is in use?	CCTV warning signs have been positioned in and around all areas covered by CCTV. The signs are reviewed annually to ensure it is fit for purpose and meet national guidelines.	

6	Is the CCTV code of Practice up to date?	The code of practices used by the Authority is updated on an annual basis or when new legislation is made available. The most recent update of the CCTV codes of practice used by the Authority was August 20.	
7	Is the CCTV code of practice accessible to staff and the public	The code of practice is readily available for all staff within the CCTV control room. Copies are available for the public use via the Stockton on Tees Borough Council website or upon request in person, telephone or email.	
8	Is the equipment of sufficient quality to enable images to be used as evidence in court?	All cameras are serviced and meet the required quality assurance requirements. The authority also considers upgrading any of its CCTV cameras as and when necessary, based on operational demand.	
9	Are there regular function checks to ensure that all equipment is in operating and recording correctly and that all images are stamped with the correct date/time?	Daily camera and recording checks are undertaken and any identified system faults are reported for repair to the maintenance contractor.	
10	What precautions are in place to ensure that data will continue to be collected e.g. in the event of a failure of power to cameras?	Power to the recorded system is protected by an Uninterrupted Power Supply (UPS) within the CCTV control room. The UPS would enable the system to be shut down in a controlled manner, allowing the maintenance supplier time to rectify any faults.	
CCTV System Review			
Requirement		Review of Compliance	Further Actions Required
1	Has the Camera Scheme been reviewed and are any installations reviewed?	The full CCTV network is reviewed yearly. All new CCTV installations go through the same review process, when installed part year.	
2	Where are the real time images from the cameras displayed?	Real time images are displayed within CCTV control room and if required specific cameras can be displayed in Police HQ.	

3	Who has operational access and ability to control the CCTV cameras?	Operational access is restricted to the system manager, supervisor, team leaders and appointed CCTV operators in compliance to CCTV codes of practice and the Protection of Freedoms Act 2012.	
4	Where are recorded images stored?	Images are stored on digital video recorders located within a secure location within the CCTV control room and are not recorded at any other off-site location.	
5	What measures are in place to control access to the area in which the recorded images are stored?	Access control measures and procedures are in place to restrict access into the control room, allowing access only to authorised and trained personnel.	
6	Who has access to the recorded images?	Access is restricted to system manager, supervisor, team leaders and appointed CCTV operators. Access as required is provided to the maintenance contractor solely for the purposes of system maintenance.	
7	How is access gained to the recorded images?	Physical access is gained by approved users via system login, controlled access in managed by the authorising officers.	
8	How long are the images retained?	31 days, any evidential Master and working copies are supplied to Police. All other authorised third-party Enforcement agencies are supplied with a working copy and the master copy is held securely for 3 years.	
9	How are the images deleted?	The system automatically over-rights all data not required for evidential purposes after 31 days. This is then checked on a random basis daily to ensure that this measure is in place and functioning.	

10	When the data is downloaded or copied for release to a third party how is information recorded?	A procedure is in place for all CCTV requests. The form must be signed and submitted before any data can be released and the details are recorded in the CD/DVD management system logging in accordance with the Police and Criminal Evidence Act.	
11	What processes are in place to ensure that data protection responsibilities are understood by persons receiving the data?	Data is only released to the Police and other enforcement agencies. These agencies are all required to have Data Protection Policies in place. Relevant paperwork is completed, and a copy retained for records. This is further covered by measures such as Information Sharing Protocols.	
Service Standards			
Requirement		Review of compliance	Further Actions required
1	Ensure that the CCTV control room is staffed by the minimum staffing levels 24 hours a day 7 days a week.	The CCTV control room was operational 24/7 for the period covering 2019/20. Staffing levels were maintained as per manning level requirements.	
2	When requested, provide CCTV evidence to Police and other enforcement agencies within 7 days of written request.	All requests were achieved within the 7-day time scale target.	
3	Meet Security Industry Authority (SIA) licensing requirements for Public Space Surveillance.	All CCTV operators hold SIA licencing licenses in both Security and CCTV. The Corporate management team hold non-front-line badges.	

4	Ensure that at least 99% of on-street CCTV cameras are fully operational at all times.	Averages of 99% of cameras were operational during year 2019/20.	
5	Provide and maintain a CCTV Code of Practice agreed by the Council and Cleveland Police.	The Codes of Practice are shared with Police colleagues annually and the last updated was July 2017.	
6	Maintain the system using an external contractor who will provide emergency call-out and repair services.	A bespoke and specific contract is in place, provided by one of the national CCTV suppliers through a tendering process.	
Home Office Surveillance Camera Code of Practice Guiding Principles And Privacy impact review			
Requirement		Review of Compliance	Further Actions Required
1	Use of a surveillance camera must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.	The operation of the Public Space Surveillance Network in Stockton on Tees is done so for a specific purpose, detailed within the Code of Practice. The Privacy impact assessment for the Scheme and new CCTV installations documents the purpose for each individual camera and this is subject to annual review.	
2	The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.	The CCTV system takes into account the impact CCTV has on a business, property, location and an individual by carrying out a yearly privacy impact review. A camera specific review is carried out for all new CCTV installations.	

<p>3</p>	<p>There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.</p>	<p>The following documents are published on the authority's website for members of the community and to show full and complete transparency:</p> <ul style="list-style-type: none"> • CCTV Code of Practice • Service Standards/Privacy Impact Review • Annual Performance Report • Surveillance Camera Code of Practice: self-assessment tool. • Contact / ownership details are also available via the website and Code of Practice. 	
<p>4</p>	<p>There must be clear responsibility for all surveillance camera system activities including images and information collected, held and used.</p>	<p>Details of responsibilities are contained within CCTV Code of Practice. Images and Information that is collated are held securely and can only be obtained via a strict monitored procedure.</p>	
<p>5</p>	<p>Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.</p>	<p>Existing systems / procedures have been in operation since 1994 and updated as and when required. CCTV Code of Practice and any additional guidelines, including operational procedure manual for control room staff are available.</p>	
<p>6</p>	<p>No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.</p>	<p>Non evidential images are system deleted after 31 days. All stored information/working copies/master copies of the CCTV evidence must be signed and collected by the officer involved on the case.</p> <p>Any non – Police Enforcement agencies are handed the working copy of any evidential images and the master is stored in the SBC control room for 3 years before being destroyed.</p>	

<p>7</p>	<p>Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.</p>	<p>All requests for the release of data shall be processed in accordance with the procedures detailed within the Code of Practice. All such requests shall be channelled through the data controller. The system owner has responsibility for oversight of this procedure.</p> <p>Primary requests to view data generated by a CCTV System are likely to be made by third parties for any one or more of the following purposes:</p> <ul style="list-style-type: none"> • Providing evidence in criminal proceedings (e.g. Police and Criminal Evidence Act 1984, Criminal Procedures & Investigations Act 1996, etc.) • Providing evidence in civil proceedings or tribunals. • The prevention of crime. • The investigation and detection of crime, this may include identification of offenders. • Identification of witnesses. <p>Access restrictions apply as detailed in the CCTV Code of Practice. All retained Images are documented and signed out by authorised personnel and third parties only.</p>	
<p>8</p>	<p>Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and</p>	<p>CCTV operators are trained to the national standard and are fully competent. This is evidenced by obtaining the SIA accredited licence for Public Space Surveillance. Annual training, supervision and appraisals help to enhance knowledge and competency</p>	

	work to meet and maintain those standards.	standards. Random checks are carried out to support / address any competency issues not picked up through direct daily supervision.	
9	Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.	Appropriate security measures are in place as detailed within the CCTV Code of Practice. All images and information are securely held within the control room. Access to such images is strictly controlled and Network video recorders are securely locked away and access to downloaded images is Controlled and signed out by authorised persons only.	
10	There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.	All legal requirements, polices and standards met, as detailed in the CCTV Code of Practice. All policies are strictly controlled by the system owner and data controller as well as duty supervisors, regular checks to ensure compliance of the polices and standards are completed. Regular reports are produced showing statistical information on footage reviews. Home office guidance is followed using the recommended principles.	
11	When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then 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.	The System has been designed to assist in the prevention and detection of crime and to support public safety. The Codes of Practice have been written and reviewed to take into account all factors.	

12	Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.	CCTV operators / supervisor's complete electronic incident reports. This information is audited, monitored for accuracy and kept up to date. All data is stored and deleted as appropriate, working to guidelines.	
----	---	--	--