Stoke-on-Trent City Council
CCTV CODE OF PRACTICE FOR CCTV SCHEME (BS 7958, BS 7858)

City of
Stoke-on-Trent

ANNEX 1

CCTV CODE OF PRACTICE

FOR CCTV SCHEME (BS 7958, BS 7858)

Contents

1. Introduction

1.1 Definitions

CCTV scheme means the totality of the arrangements for closed circuit television in the locality and includes the CCTV system, staff and operational procedures.

CCTV system means the surveillance items comprising cameras and associated equipment for monitoring, transmission and controlling purposes, for use in a defined zone.

Control Room means the secure area of a building where CCTV is monitored and where data is retrieved, analysed and processed.

Data Protection Laws means the Data Protection Act 2018 or any successor legislation and (for so long as and to the extent that the law of the European Union has legal effect in the UK) the General Data Protection Regulation (*(EU) 2016/679*) and any other directly applicable European Union regulation relating to privacy.

Incident is an activity that raises cause for concern that the safety or security of an individual or property including vehicles may be compromised or that an offence has been, is being or is about to be, committed, or that an occurrence has taken place warranting specific action by an Operator.

Manager means the CCTV Manager, or, another Council officer authorised to act on his behalf.

Operators are employees of Stoke-on-Trent City Council 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.

Owner means Stoke-on-Trent City Council.

Personal Data means data which relates to a living individual who can be identified:

- from that data or
- from that data in combination with other information.

1.2 Scope of the Scheme

Stoke-on-Trent City Council ('the Council') operates a Closed Circuit Television ('CCTV') scheme. The System comprises of cameras located in specific external and internal locations within the Council's area, with control, monitoring and recording facilities based at the Council's CCTV Control Room.

The intellectual property rights in relation to any material created as part of, or for the purpose of, the CCTV scheme (including CCTV footage) shall vest in the Council.

1.2 System Description

The System consists of static and fully functional (pan, tilt and zoom) cameras and either a fibre optic or other transmission system which sends images to the Control Room.

Images from all cameras are recorded simultaneously throughout a 24 hour period 365 days each year.

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.

1.3 Amendments to the Code

Major changes to this code will take place only after consultation with the relevant management group.

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

- matters which have privacy implications
- additions to permitted uses criteria e.g. purposes of the CCTV scheme
- changes in the right of access to personal data, except statutory requirements
- significant legal implications.

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

- additional clarifications, explanations and corrections to the existing code
- amendments to the code of practice in order in light of legislative changes

Minor changes may be made by the Manager who will communicate the revised code to all relevant members of staff.

A copy of the Code of Practice will be made available to the public on request.

1.4 Supplementary Documentation

The Code of Practice will be supplemented by the following documents:

- CCTV Operations Procedural Manual
- Operators Equipment manual

Each document contains instructions and guidance to ensure that the objectives and principles set out in this Code of Practice are achieved. The two supplement documents will be restricted to the partners and staff members only.

2 Purpose and Compliance

2.1 Purpose of the CCTV scheme

The CCTV scheme has been established for the following purposes:

(a) reducing the fear of crime/offences
(b) deterring and preventing crime/offences
(c) improving the safety and security of residents, visitors and the business community who use the facilities within the areas covered
(d) assisting in the maintenance of public order and reducing offences involving vandalism and nuisance
(e) providing high quality evidence which may assist in the detection of crime and the apprehension and prosecution of offenders
(f) protecting property
(g) providing assistance with civil claims
(h) providing assistance with issues relating to public safety and health
(i) providing assistance and reassurance to the public in emergency situations

2.2 Purpose of the Code of Practice

This Code of Practice has been drafted to promote public confidence by developing a safe and secure environment for the benefit of those employed, visiting or using the facilities of the areas covered by the CCTV system.

The Code of Practice has a dual purpose, in that it will assist operators and other staff involved in the use of the CCTV scheme to understand their obligations whilst reassuring the public that appropriate safeguards exist.

2.3 Compliance with the Codes of Practice

The Council is committed to compliance with this Code and will also have regard to:-

- the Surveillance Camera Code of Practice ('the SC Code') https://www.gov.uk/government/publications/surveillance-camera-code-of-practice
- the Information Commissioner's Office Code of Practice ('the ICO Code') https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf
- and British Standards

The Manager, CCTV Operators and users of the CCTV systems and associated safety and security equipment connected to the Control Room 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.

CCTV Operators, users and any visitors to the Control Room 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 Principles of Operation

3.1 Right of Privacy

The Council will ensure that the CCTV scheme is operated in accordance with the principles and requirements of the Human Rights Act 1998, in particular Article 8 which provides the right to respect for private and family life.

3.2 General Principles of Operation

Prior to its installation and use, a camera system must have a clearly defined purpose which is in pursuit of a legitimate aim and it must be necessary to meet an identified pressing need. It should only be used for the specific purpose which it is established to address.

Therefore prior to the installation of cameras, a Data Protection Impact Assessment will be undertaken in compliance with the SC Code and the ICO Code. It should take into account the nature of the problem the proposed system is seeking to address, whether a surveillance system is justified and effective, whether better solutions exist, what effect its use may have on individuals and whether, in light of this, its use is a proportionate response.

This ensures that the system is justifiable and there is consultation with those most likely to be affected with appropriate safeguards for the impact on their privacy. This also demonstrates that the necessity and extent of any interference with Article 8 of the Human Rights Act 1998 has been considered.

The SC Code states that any deployment that includes audio recording is likely to require strong justification of necessity to establish its proportionality.

The cameras are sited to capture images which are relevant to the specified purposes for which the CCTV scheme has been established as set out in 2.1. Cameras are sited to ensure that they can produce images of the right quality, taking into account technical and environmental issues. To accomplish this, an 'Operational Requirement' will be completed at the time of the 'Data Protection Impact Assessment' for each proposed camera to dictate the quality of images required.

Help Points may be used in conjunction with the cameras.

If wireless transmission systems are used to control CCTV equipment, sufficient safeguards will be in place to protect them from being intercepted.

The CCTV 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.

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

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

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

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

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

3.3 Signage

The CCTV scheme aims to provide surveillance of the public areas within the Stoke-on-Trent City Council area in order to fulfill the stated purposes of the scheme. The area protected by CCTV will be indicated by the presence of signs. The signs will be placed so that the public are aware that they are entering a zone which is covered by surveillance equipment. The signs will state that the Council is responsible for the CCTV scheme, the purposes of the CCTV scheme and a contact telephone number.

3.4 Point of contact

Should the public wish to make contact with the owner of the CCTV scheme they may write to:

The CCTV Operations & Development Manager
City of Stoke-on-Trent
The Regent Centre
Regent Road
Hanley
Stoke-on-Trent
ST1 3EG

The contact point will be available to members of the public during office hours. Enquirers will be provided with the relevant documentation.

3.5 Annual review of the CCTV scheme

There will be an annual review of the CCTV scheme covering the following aspects:

a) ensuring the camera systems remain necessary, proportionate and effective in meeting their stated purpose for deployment

b) Assessing whether the location of the cameras remains justified in meeting the stated purpose and whether there is a case for removal or relocation
c) whether the purpose and objectives statements remain valid
d) change in extent of the CCTV scheme
e) contracts with suppliers
f) a review of the data protection or legal requirements
g) maintenance schedule and performance test of the system
h) CCTV scheme evaluation findings
i) complaints procedure and evaluation

As part of the annual review of the CCTV scheme, there will also be an annual review of this Code. In addition, the Code will be kept up to date with changes in legislation and procedure as and when they occur.

The officer responsible for the annual review of this Code is the CCTV Manager.

3.6 Storage

Data from the CCTV System is stored in accordance with the retention period set out at 3.6 of this Code. Only authorised personnel in the Control Room can access the data and a record must be made detailing the date/time of access and the purpose. Data from the CCTV system should be stored in such a way that maintains the integrity of the image and information with particular importance attached to ensuring that meta data is recorded reliably and compression of data does not reduce its quality.

3.7 Retention Period and Deletion

Any data captured as part of the CCTV scheme should not be kept for longer than necessary to fulfil the purpose for which they were obtained in the first place. Generally, the Council will retain CCTV images and information for 31 days from the date it was captured, unless required for evidential purposes or if a Subject Access Request is received which may require footage to be retained beyond the ordinary retention period. Where the nature of a particular CCTV system requires a different retention period, this will be specified in the individual operating procedures for the system. Once the retention period has passed, data will be erased. Data will not be held for longer than necessary.

4 Legislative Framework

4.1 Data Protection

For the purpose of the CCTV scheme, the Council is the Data Controller. The Council is registered with the Information Commissioner's Office, Registration Number: Z5110678. The CCTV scheme will be managed in accordance with the principles of the Data Protection Laws which encompass six data protection principles, as follows:

First Data Protection Principle

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals

Second Data Protection Principle

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

Third Data Protection Principle

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

The Fourth Data Protection Principle

Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

The Fifth Protection Principle

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals

The Sixth Data Protection Principle

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful

processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

The Accountability Principle
As the Data Controller, the Council shall be responsible for, and be able to demonstrate compliance with the other data protection principles.

4.2 Human Rights Act 1998

The Council has considered the wider human rights issues and in particular the implications of the Human Rights Act 1998, Article 8 (the right to respect for private and family life).

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. 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.

Any infringement by a public authority of another's rights must be in pursuit of a legitimate aim, proportionate and compliant with any relevant legal obligations.

4.3 Freedom of Information Act 2000

As a public authority, the Council is required to comply with requests for information submitted under the Freedom of Information Act.

If a request for images is received and the person requesting is the data subject, these will be exempt from the FOIA and will be dealt with under the subject access regime as set out in Data Protection Laws. Any other requests where the requester is not the data subject can only be disclosed if it does not breach Data Protection Laws. Such requests would need to be sent to the Council's Information Rights Team.

4.4 Regulation of Investigatory Powers Act 2000 (RIPA)

RIPA allows the Council, as a local authority, to undertake covert surveillance, provided that it is in accordance with RIPA procedure, limitations and criteria set out in the formal documentation that must be used.

The use of overt CCTV cameras by the Council would not normally require an authorisation under RIPA as members of the public should be made aware that such systems are in use. For example, by virtue of cameras or signage being

clearly visible, through the provision of information and by undertaking consultation. However, where overt CCTV or other overt surveillance cameras are used in a covert and pre-planned manner as part of a specific investigation or operation, for the surveillance of a specific person or group of people, a directed surveillance authorisation should be considered. In this regard, the Council's RIPA policy will be consulted which details the authorisation procedure.

4.5 Surveillance Camera Code of Practice (the SC Code)

The SC Code was issued under section 30 of the Protection of Freedoms Act 2012 and sets out guidelines for surveillance camera systems to ensure that individuals and wider communities have confidence that surveillance cameras are deployed to protect and support them.

The SC Code has been built upon 12 guiding principles, which provide a framework of good practice that the Council must have regard to when exercising any of its functions to which the SC code relates. In particular, the SC Code states that the use of a surveillance camera system must:

- Always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
- Take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified
- Have as much transparency as possible, including a published contact point for access to information and complaints.
- Have clear responsibility and accountability for all surveillance activities including images and information collected, held and used.
- Have clear rules, policies and procedures in place and these must be communicated to all who need to comply with them.
- Have no more images and information stored than that which is strictly required and ensure such images and information are deleted once their purposes have been discharged.
- Restrict access to retained images and information with clear rules on who can gain access.
- Consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
- Be subject to appropriate security measures to safeguard against unauthorised access and use.
- Have effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with and ensure regular reports are published.
- when used in pursuit of a legitimate aim, and there is a pressing need for its use, 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.

- 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 Governance and Accountability

5.1 Accountability

The Council supports the principle that the community at large should be satisfied that the Public surveillance CCTV systems are being used, managed and controlled in a responsible and accountable manner and that in order to meet this objective there will be independent assessment and scrutiny. The Council is committed to maintaining a continuous review of its integrity, security, procedural efficiency, methods of operation and retention and release of data.

The Single Point of Contact for the Council is the CCTV Manager.

5.2 Roles and Responsibilities

Senior Responsible Officer (SRO)

For the purpose of this Code of Practice, the Council's Senior Responsible Officer is the Assistant Director – Governance (Monitoring Officer).

The role of the SRO is to deliver a corporate approach to the Council's responsibilities arising from the Protection of Freedoms Act 2012. The SRO has strategic responsibility for the integrity and efficacy of the processes in place within the local authority which ensure compliance with section 33 of the Protection of Freedoms Act 2012 and in respect of all relevant surveillance camera systems operated by the Council.

The Manager

For the purpose of this Code of Practice, the Council's Manager is the CCTV Manager.

The Manager 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 Senior Responsible Officer. To facilitate this, regular minuted meetings will be held to go through the points listed below:-

The Manager has responsibility for the following:-

- Communication of rules, policies and procedures to all users as part of their induction and ongoing training
- Staff management
- Observance of the policy and procedural practices
- Release of data to data subjects and third parties where appropriate and in compliance with all relevant legislation

- 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
- Development and operation of the System including ensuring there is appropriate consultation and transparency over its purpose and for reviewing how effectively it meets its purpose
- Maintenance of the quality of recording and monitoring equipment
- Proactive checks on a regular basis to ensure that procedures (including the retention period) are being complied with
- Regularly checking that the time and date stamp on images is correct e.g. when the UK switches between summer and winter time
- Regular maintenance regime to ensure the system produces high quality information
- Ensuring any wireless transmission is suitably secure and encrypted where appropriate

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 CCTV scheme comply with the Code of Practice and Procedural Manual. Dealing with breaches of the codes and disciplinary measures shall lie with the manager.

The manager shall produce a written policy and be responsible for its implementation. The manager 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 manager shall be accountable to the Senior Responsible Officer and will provide periodic progress reports on the CCTV scheme. The manager/supervisor will resolve technical and operational matters.

The Supervisor

The supervisor has a responsibility to ensure that at all times the system is operated in accordance with the policy and all procedural instructions relating to the system, and for bringing to the immediate attention of the manager any matter affecting the operation of the system, including any breach or suspected breach of the policy, procedural instructions, security of data or confidentially. In the Managers absence the Supervisor will have responsibility for all of the tasks listed above as being the responsibility of the Manager:

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 CCTV scheme. This will include regular checks and audit trails to ensure that the documentation systems in place are working effectively. These systems include:

- The video image log
- The operators log
- The incident log
- Witness statements
- Faults and maintenance log
- The security of data
- Audit logs
- Authorisation of visitors – to be checked & counter signed by the Supervisor

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

The Operators

The operators will be responsible for complying with this Code, the CCTV Operations Procedural Manual and the Operators Equipment manual.

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

Failure by 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 Council's policy.

5.3 Annual Assessment

It is a recommendation of the Surveillance Camera Commissioner and the Information Commissioner that the CCTV system should be reviewed annually to determine whether CCTV continues to be justified.

An annual assessment of the CCTV scheme will be undertaken by an independent consultancy appointed by the owner to evaluate the effectiveness of the system. This will include annual reviews of the CCTV 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 CCTV scheme. If the CCTV scheme is not achieving its purpose modification and other options will be considered.

5.4 Audit

An independent audit should be conducted to monitor the CCTV scheme. This should include annual reviews of the CCTV scheme's operation and working practices and, where appropriate, recommendations for improvements.

An independent audit should be conducted before the publication of the annual report. This audit should consider the following:

a) the level of attainment of objectives and procedures;
b) random audits of all logs and the release of information;
c) the review policy; and
d) standard costs for the release or viewing of material.

5.5 Annual Report

An annual report will be prepared for CCTV schemes monitoring public spaces. This report should be made available to the public.

The report will include the following details:

a) a description of the CCTV scheme and the geographical area(s) of operation;
b) the CCTV scheme's policy statement;
c) the objective and scope of the CCTV scheme;
d) any changes to the operation or management of the CCTV scheme;
e) any changes that have been made to the policy;
f) any proposals to expand or reduce the operation of the CCTV scheme; and
g) the CCTV scheme's aims and objectives for the next 12 months.

The report should also provide details of the CCTV scheme's achievements during the previous 12 months, which might be based on information already held by the CCTV scheme. The details of the CCTV scheme's performance should include:

1) the number of incidents recorded by the CCTV scheme;
2) the number of incidents reported to the law enforcement agencies and, where appropriate, other bodies, e.g. the local authority;
3) an assessment of the CCTV scheme's impact on crime levels and types of crime in the area covered by it; and
4) an assessment of the CCTV scheme's impact on its objectives, including:

- the number of Data Protection Impact Assessments completed;
- the number of reviews of footage by police and authorised agencies; and
- the number of incidents per camera for the previous twelve months.

The results will be assessed against the stated purposes of the CCTV scheme. If the CCTV scheme is not achieving its purpose, modification and other options will be considered. The results of the assessment will be made available by the Council.

The above are requirements of British Standard 7958, the Information Commissioner's CCTV Codes of Practice and Surveillance Camera Commissioner's Code of Practice.

5.6 Complaints

A member of the public wishing to make a complaint about the system may do so through the Council's complaint procedure by making a complaint to the

Customer Feedback Team
Floor two
Civic Centre
Glebe Street
Stoke-on-Trent, ST4 1HH

Email: customer.feedback@stoke.gov.uk

5.7 Personnel

Security screening

All personnel employed to control/operate or manage the CCTV scheme will be security screened in accordance with British Standard 7858: Code of practice for screening of personnel in a security environment.

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 recognized qualifications
- Recognise and understanding privacy and disclosure issues
- The disciplinary policy

Contractors

There are special conditions imposed upon contractor’s carrying out works on the system. These are detailed in the Procedural Manual. It should be noted that wherever possible contractors should not have sight of any recorded data.

6 Control Room Management and Operation

6.1 Access to Control Room

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

Only those persons with a legitimate purpose will be permitted access to the Control Room.

The Manager or in his/her absence the Supervisor, 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 or collecting/returning media being considered for intelligence or evidential purposes. These visits will take place by prior appointment
Engineers and cleaning staff (These people will receive supervision throughout their visit)
Independent Inspectors appointed under this Code of Practice may visit the control room without prior appointment
Organised visits by persons authorised by the Manager in controlled circumstances.

All visitors to the monitoring area, including Police Officers, will be required to sign a visitor log and a declaration of confidentiality.

6.2 Response to an incident

The Procedural Manual details:
What action should be taken
Who should respond
The time scale for response
The times at which the observation should take place

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.

6.3 Who makes the response and the timescale

Incidents of a criminal nature will be reported to Staffordshire Police. The response will be made by the Police Service in accordance with their policies.

6.4 Observation and recording of incidents

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 and the operator will activate real time recording.

6.5 A successful response

The criteria for measuring a successful response are:

- A good observational record of the incident
- A short time scale for response to the incident
- Identification of a suspect
- The prevention or minimisation of injury or damage
- Reduction of crime and disorder
- Improving public safety
- Restoration of tranquillity

6.6 Operation of the System by the Police

Under certain circumstances the Police may make a request to remotely observe 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 control.

In the event of the police requesting use of the equipment from within the CCTV control room to monitor situations, such a request will only be permitted on the request of a Superintendent or his designated deputy and only with the permission of the System manager or his designated deputy. The request should be in writing, however, in emergencies this can be a verbal request which should then be followed by the written request as soon as practicable. 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.

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 Superintendent (or designated deputy).

Once the police undertake any of the above they become a Data Controller and have responsibilities as set out in Data Protection Laws.

A radio/telephone link through to the police station is available to effectively relay information on incidents that arise.

7 Privacy and Disclosure Issues

7.1 Privacy

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 any residential properties. If it is found there is a possibility that cameras would intrude in private areas, privacy zones would be programmed into the cameras where possible and/or CCTV operators trained to recognise privacy issues.

7.2 Disclosure Policy

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 will not be retained longer than necessary. However, on occasions it may be necessary to retain images for longer periods, 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) Monitors displaying images from areas in which individuals would have an expectation of privacy will not be viewed by anyone other than authorised employees.
d) Recorded material will only be used for the purposes defined in the objectives and policy.
e) Access to recorded material will be in accordance with policy and procedures.
f) Information will not be disclosed for commercial purposes and entertainment purposes.
g) All access to the medium on which the images are recorded will be documented.
h) 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.
i) Viewing of the recorded images should take place in a restricted area.

7.3 Access to recorded images

Access to recorded images will be restricted to the manager who will decide whether to allow requests for access by third parties in accordance with all applicable legislation.

7.4 Viewing recorded images

Viewing of recorded images should take place in a restricted area. Other employees should not be allowed to have access to that area when viewing is taking place. An audit trail must be kept to include details of who has viewed the images, the date and time, and the purpose.

7.5 Operators

All operators are trained in their responsibilities in relation to access to privacy and disclosure issues however it is only the Manager who is able to make the decision whether or not to disclose data.

7.6 Removal of medium for Viewing

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

7.7 Access to data by third parties

Access to images by third parties will only be allowed in limited and prescribed circumstances. It is anticipated that disclosure could be required in the following situations:-

- Law enforcement agencies where the images recorded would assist in a specific criminal enquiry
- Prosecution agencies
- Legal representatives
- The media, where it is assessed by the Police that the public's assistance is needed in order to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. As part of that assessment the wishes of the victim of an incident should be taken into account.
- The people whose images have been recorded and retained (Data Subject) subject to compliance with Data Protection Laws.

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

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

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.

If it is intended that the images will be made more widely available, that decision should be made by the manager and the reason documented.

Where the Council discloses data, the method should be secure to ensure that the data is only seen by the intended recipient and appropriate records maintained. Where images are disclosed, consideration should be given to whether images of individuals may need to obscured to prevent unwarranted identification.

Where information is disclosed, the date of disclosure should be recorded along with details of who the info has been provided to (the name of the person and the organisation) and the reasons for this.

7.8 Disclosure in the public interest

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

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

7.9 Data subject access disclosure

All staff involved in operating the equipment must be able to recognise a request for access to recorded images by data subjects and be aware of individual's rights under this section of the Code of Practice and that the Council only has one calendar month to meet their obligations. Where a member of staff receives a Subject Access Request, they must notify the Manager immediately.

Individuals whose images are recorded have a right to view the images of themselves and, unless they agree otherwise, to be provided with a copy of the images. This must be provided without undue delay and, at the latest, within a month of receiving a request.

Data subjects requesting access will be provided with a standard subject access request form (Appendix 'A') and accompanying leaflet (Appendix 'B') describing the types of images recorded and retained and the purposes for recording and retention. It should be noted however, that individuals may submit their request in another format, e.g. by letter or verbally, although they should always be encouraged to make a written request.

If images of third parties are also shown with the images of the person who has made the access request, consideration will be given as to whether there is a need to obscure the images of third parties. Data Protection Laws mean that the Council does not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if the other individual has consented to the disclosure or it is reasonable to comply with the request without that individual's consent.

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 to enable the Council to locate the requested data, the data subject will be advised, as soon as possible, that more information is required from them before responding to their request. A written response must be provided within one calendar month of receipt of the request or one month

from the date that any further information requested has been received. If a request is complex or more than one is made, the response time may be a maximum of three calendar months, starting from the day of receipt. If an individual refuses to provide any additional information, the Council must still endeavour to comply with the request i.e. by making reasonable searches for the information covered by the request.

Details of all subject access requests will be documented including, if a subject access request is not to be complied with, the reason for the refusal will be documented.

7.10 Provision of data to the individual

The Manager, having verified the validity of a request, should provide requested material to the individual. Where a decision has been made that third parties should not be identifiable, then arrangements will be made to disguise or blur the images in question. It may be necessary to contract this work out to another organisation. Where this occurs, there will be a written contract with the processor which specifies exactly how the information is to be used and the provision of explicit security guarantees. The procedure outlined in Stoke-on-Trent City Council's Procedural Manual will be followed.

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

The Data Subject should also be provided with details of the ICO website and details of how to complain if they feel the Council has failed to comply with the requirements of the ICO's code.

7.11 Other rights

All staff involved in operating the equipment must be able to recognise a request from an individual to exercise a right under the Data Protection Laws and the Manager should be notified immediately.

7.12 Media Disclosure

Disclosure of images from the CCTV system must be controlled and consistent with the purpose for which the system was established. For example, if the system is established to help prevent and detect crime it will be appropriate to disclose images to law enforcement agencies where a crime needs to be investigated or to the media for identification purposes or, on some occasions, where the Council wants to make examples of some activity public, which may involve redacted images where appropriate.

8 Recorded Material Management

8.1 Retention of Images

Images will not be retained for longer than is necessary. While images are retained, access to and security of the images will be controlled in accordance with the requirements of Data Protection Laws.

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

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

Recorded material will not be released to organisations outside the ownership of the system unless it would comply with Data Protection Laws.

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

8.2 Quality and Maintenance

In order to ensure that clear images are recorded at all times the equipment for making recordings and any 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.

8.3 Digital Recordings

In a digital CCTV system, where possible, the register should show the life of the recorded 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);
time/date/person removing medium from secure storage for use;
time/date/person returning medium 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.

Details of all reviews of images, including persons present, the purpose, the date/time and results of such review.

8.4 Making Recordings

Details of the recording procedures are given in the Procedural Manual.

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

8.5 Video Prints

Video prints will only be made when absolutely necessary. Those video prints not handed to the police will be retained in a secure cabinet until destruction is authorised. The taking of video prints will be recorded in a register to be retained in the control room.

9 Documentation

9.1 Logs

Log books must be sequential in order that pages or entries cannot be removed and full and accurate records kept.

An accurate log of operator working times will be maintained. Each operator will maintain a log of any event or occurrence including:

a) change of operator identifying the operator on duty at that workstation and showing that:
   - that the correct time was being displayed
   - that the recording equipment appeared to be operating correctly
b) incidents including details of time, date, location, nature, name of operator dealing and action taken
c) routine camera patrols, whether taken manually or through the utilisation of pre-set times
d) Privacy zones, detailing where, for any reason, it is necessary to encroach on private areas that are not part of the contractual patrol
e) public address use

9.2 Administrative documents

The following shall be maintained:

- video/digital tracking register
- occurrence/incident Book
- visitors register
- maintenance of equipment, whether routine or breakdown
- staff signing on and off duty
- video print log
- list of installed equipment

Appendix A

Subject Data Access 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.

Your Rights
Subject to certain exemptions, you have a right to be told whether any personal data is held about you and to receive a copy of the information in a permanent form. To protect your security Stoke-on-Trent City Council will only provide 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 Stoke-on-Trent City Council is not obliged to comply with an access request unless –

- The other individual has consented to the disclosure of information, or
- It is reasonable in all the circumstances to comply with the request without the consent of the other individual(s)

Stoke-on-Trent City Council CCTV System Rights
Stoke-on-Trent City Council may deny access to information where the Act allows or does not apply. The main exemptions in relation to information held on the CCTV System are where the information may be held for

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

Section 1 Asks you to give information about yourself that will help us confirm your identity.

Section 2 Asks you to provide evidence of your identity by producing TWO official documents (which between them clearly show your name, date of birth and current address) together with a recent full photograph of you.

Section 3 The declaration must be signed by you.

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

Head of Service
Stoke-on-Trent City Council
The Regent Centre, Regent Road
Hanley
Stoke-on-Trent

SECTION 1 About Yourself

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

PLEASE USE BLOCK CAPITAL LETTERS

Title *(tick box as appropriate)*	Mr		Mrs		Miss		Ms	
Other title *(e.g. Dr., Rev., etc.)*								
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)*	
	Post Code
A telephone number will be helpful in case you need to be contacted.	Tel. No.

SECTION 2 Proof of Identity

To help establish your identity your application must be accompanied by TWO official documents that between them clearly show your name, date of birth and current address.

For example: a birth/adoption certificate, driving license, medical card, passport or other official document that shows your name and address.

Also a recent, full face photograph of yourself.

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

SECTION 3 Supply of Information

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

(a)	View the information and receive a permanent copy	YES /
(b)	Only view the information	YES /

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 guilty of an offence.

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

SECTION 5 To Help us Find the Information

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

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

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

Were you: (tick box below)	
A person reporting an offence or incident	
A witness to an offence or incident	
A victim of an offence	
A person accused or convicted of an offence	

Other – please explain	

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

Before returning this form	• Have you completed ALL Sections in this form?
Please check:	• Have you enclosed TWO identification documents? • Have you signed and dated the form?

Further Information:

These notes are only a guide. The law is set out in the Data Protection Act 2018, obtainable from The Stationery Office. Further information and advice may be obtained from:

The Office of the Information Commissioner
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire, SK9 5AF

Please note that this application for access to information must be made direct to **Stoke-on-Trent City 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? ☐

Details of 2 Documents (see page 3)

Documents Returned? ☐

Member of Staff completing this Section:

Name ☐ Location ☐

Signature ☐ Date ☐

Appendix B

CCTV SCHEME LEAFLET

The Data Protection Act 2018

CCTV IN OPERATION

This brochure contains advice and information regarding data recorded by the CCTV system and gaining access to that data.

The CCTV Operations & Development Manager
City of Stoke-on-Trent
The Regent Centre
Regent Road
Hanley
Stoke-on-Trent
ST1 3EG

THE PURPOSES FOR WHICH IMAGES ARE RECORDED

Full details of the principles and criteria under which this system operates may be found in the CCTV Code of Practice.

The following purposes have been established for the Stoke-on-Trent City Council CCTV Scheme:

(a) reducing the fear of crime/offences
(b) deterring and preventing crime/offences
(c) improving the safety and security of residents, visitors and the business community who use the facilities within the areas covered
(d) assisting in the maintenance of public order and reducing offences involving vandalism and nuisance
(e) providing high quality evidence which may assist in the detection of crime and the apprehension and prosecution of offenders
(f) protecting property
(g) providing assistance with civil claims
(h) providing assistance with issues relating to public safety and health
(i) providing assistance and reassurance to the public in emergency situations

10 CODE OF PRACTICE

Copies of the Code of Practice are available free of charge on application to the CCTV System Manager.

RECORDED IMAGES

The CCTV system operates 24 hours per day, every day of the year. All cameras are continuously recorded in time lapse mode. Additional recordings may be made of individual camera pictures in either real time mode.

All recordings are retained for a minimum of 31 days. If no legitimate request for retention of the recording has been made and there is no other valid reason to retain it for longer it is then erased. All requests for retention of recordings are considered against the provisions of the Data Protection Act, Human Rights Act and the Code of Practice.

The storage, processing and use of the recorded data obtained by the CCTV system is guided by the following general principles.

Recorded data will only be used for the purposes defined in the Code of Practice and in accordance with the provisions of the Data Protection Act and Human Rights Act.

Access to recorded data shall only take place in the circumstances defined in the Code of Practice and the provisions of the relevant legislation.

Recorded data will not be sold or used for commercial purposes or the provision of entertainment.

The showing of recorded data to the public will only be permitted in accordance with the law.

Data released shall remain the property of Stoke-on-Trent City Council.

DISCLOSURE POLICY

Disclosure of data obtained by the CCTV System is only permitted in accordance with the relevant legislation and the criteria contained within the Code of Practice.

SUBJECT ACCESS

If you wish to exercise your rights of subject access as provided for in the Data Protection Act 2018 and GDPR you will be asked to make the request in writing on a standard subject access request form.

All requests for subject access will be dealt with by the CCTV Manager or a nominated deputy. A written response will be provided within one calendar month of receipt of the request or one month from the date that any further information requested has been received. If your request is complex or you make more than one, the response time may be a maximum of three calendar months, starting from the day of receipt.

The Information Commissioner's Office has published a Code of Practice for Users of public area CCTV Systems. A copy of this code may be obtained from ico.org.uk or on application to the Information Commissioner.