Darlington Borough Council

Closed Circuit Television

Code of Practice

For the operation of public space CCTV systems, including re-deployable systems, Body Worn Video and Council owned buildings.

Approved by Cabinet 7 January 2014
Updated 27 October 2020

Table of Contents

Code of Practice

1. INTRODUCTION

This Code of Practice is to control the management, operation and use of all Close-Circuit Television (CCTV) systems under the control of Darlington Borough Council, and is used in conjunction with the Home Office Surveillance Camera Code of Practice pursuant to section 29 of the Protection of Freedoms Act 2012.

The Council will retain ownership of all recorded material in various formats, including, Compact Disc (CD), Digital Versatile Disc (DVD), Universal Serial Bus (USB), external HDD and hard copy print, and retains absolute copyright of any recorded material. For the purpose, of this document, any recorded material will be referred to as 'video imagery'. The Council will not release video imagery for commercial purposes or for the provision of entertainment. Video imagery will only be released for the purposes of evidence and on occasions education and training purpose.

The day-to-day operation of the Council's systems will be the responsibility of the CCTV Team within the Community Safety Service. The CCTV systems operate 24 hours a day, 365 days a year, except in cases of maintenance/upgrades, faults etc, where it may be necessary for a particular system to be powered down for a period of time.

It is a condition of acceptance as a partner that users of CCTV demonstrate commitment to operate in accordance with this code by signing the required Certificate of Agreement in this document. Each participant in the scheme is bound by this Code of Practice and any subsequent amendments thereto.

2. TERMS AND DEFINITIONS

For the purposes of British Standards the terms and definitions given in BS EN 62676 suite of standards apply, together with the following.

CCTV Scheme
Totality of arrangements for CCTV in a locality including but not limited to the technological system, staff and operational procedures.

Retrieval System
A CCTV system having the capability in any medium of effectively capturing data that can later be retrieved, viewed or processed.

CCTV System

Surveillance items comprising of cameras and all associated equipment for monitoring, transmission and controlling purposes, for use in a defined area.

Distributed System
Sub system, any part of which may be linked temporarily or permanently for remote monitoring within the CCTV system.

Data
All information collected by the CCTV systems, including personal data.

Incident
An activity that has been identified as an offence that has been committed or an occurrence that has taken place that warrants further specific action from either the Police or from the Council or other third parties as the Council sees fit such as Insurance companies or solicitors. For the purposes of this scheme an incident is defined as:

> **Any event or occurrence monitored by a controller/system in respect of which information needs to be passed to another source to generate a response.**
> OR
> **A request by an authorised persons or body to monitor specific events or activity in accordance with the purposes and key objectives of the scheme.**

The provisions of the Regulation of Investigatory Powers Act (RIPA) 2000 may be relevant to such requests.

Owner
Legal person or entity, agency or individual designated and trained as having direct responsibility for the implementation of the policies, purposes and methods of control of a CCTV scheme, as defined by the owner of the scheme.

Manager
The CCTV and Security Manager has direct responsibility for the implementation of the policies, purposes and methods of control of a CCTV scheme, as defined by the owner of the scheme.

CCTV Duty Manager
Person specifically designated, trained and authorised by the owner of a scheme to ensure that at all times the system is operated in accordance with the Code of Practice and any procedural instruction issued by the owner or Manager.

Operator
Person specifically designated and authorised by the owner of a CCTV scheme to carry out physical operation of controlling that system.

Recording Material (e.g. CD/DVD/USB)
Any medium that has the capacity to store data, and from which data can later be recalled, irrespective of time.

Recorded Material
Any data that has been recorded on any medium that has the capacity to store data and from which data can later be recalled irrespective of time.

Hard Copy Print
Paper copy of a still image or images which already exist on recorded material.

Privacy Masking
The common term covering the need to restrict what can be seen by means of CCTV. It applies equally to images displayed in real time for surveillance purposes and images recorded for later use.

Directed Covert Surveillance
This is defined under section 26 of the Regulation of Investigatory Powers Act (RIPA) 2000. It relates to covert surveillance for specific purposes where the gathering of private information is a likely outcome.

3. BACKGROUND

Darlington Borough Council has and is continuing to install CCTV systems some of which are capable of expansion. Cameras have been installed within specific target areas which have been identified through the gathering of information, including the use of local public information, Crime Pattern Analysis and the Council's CCTV Decision Matrix Tool.

Community Safety is defined as any intervention that deals with anti-social behaviour and fear of crime, which may affect the quality of life of individuals and the local community. The Crime and Disorder Act 1998 defines anti-social behaviour as behaviour which causes, or is likely to cause alarm, harassment or distress to one or more persons not of the same household.

4. AIMS OF DARLINGTON BOROUGH COUNCIL'S CCTV

- Help secure safer areas and environments for those who visit, work in, trade in or enjoy leisure pursuits within the district.
- The Council's CCTV schemes will be operated fairly and lawfully and will only be used for the purposes for which they were established, or subsequently agreed in accordance with this code.
- The Council will regularly monitor, review and enhance its CCTV schemes in order to ensure and improve their effectiveness.

5. PURPOSES OF DARLINGTON BOROUGH COUNCIL'S CCTV

Darlington Borough Council's CCTV schemes exist in order for us to record, view, and occasionally monitor activity within the intended area of coverage. Safeguards are used within the systems' capabilities to ensue cameras cannot be focused within private areas, such as windows, where there is no public access. Where it is unavoidable to have a camera focused on a home or other private area as part of a larger point of focus, privacy masking will be used to cover the private area from view. This will minimise collateral intrusion.

6. COUNCIL CCTV OBJECTIVES

- The introduction of a central hub for all DBC CCTV matters. (Based within the Safety section), also referred to as SPOC (Single Point of Contact)
- Manage our CCTV responsibility by providing a compliant delivery of service through the implementation of robust CCTV processes and guidelines.
- Provide high quality evidence which may be used to further an investigation by the Council or third parties as well as law enforcement agencies to prosecute offenders.
- All schemes to be made 'fit for purpose' through preventative and reactive maintenance plans and regular operational requirement reviews.
- Effectively manage the public and third-party perception of CCTV including 'unrealistic expectations'.
- Monitor environmental conditions.
- To provide transparency to the public on how, why and where CCTV is being utilised, successes and outcomes along with other information members of the public may wish to know. Much of our CCTV information can be readily found through our Council's CCTV website page.

Every effort is made in the planning and design of the Council's CCTV systems to provide maximum effectiveness within the current area of coverage or such additional areas which may subsequently form part of the system. It is not possible to guarantee the system will be able to see or provide evidence for every incident that may occur within the target area.

7. REVISION AND ALTERATIONS TO THE CODE OF PRACTICE

This Code of Practice will be regularly reviewed, and any required revisions and alterations will then be made.

8. PLANNING OF CCTV SYSTEMS

In planning the installation of CCTV systems, Darlington Borough Council refers to a number of standards and documents in order that the passport to compliance is adhered to.

Locations of cameras (See appendix 1)

All locations where cameras are to be installed will be assessed using various relevant statistics and analysis gathered from various sources, including Police, local communities and local businesses to ensure maximum effectiveness and productivity.

Signage (See appendix 2)

Corporate signs will be installed in and around the areas covered by the Council's CCTV systems. The placing of such signs is an important aspect of the principles of the Data Protection Act 1998. They will be of an appropriate size to the location and will contain the following information:

a) The purpose of the scheme
b) What the Council intends to do with the information gathered i.e. prosecute offenders
c) Who owns the scheme
d) Contact details
e) Carry relevant Council logo's and CCTV symbol

The signs will read, or variations of this type:

'CCTV cameras are in operation 24 hours a day.
Images are being recorded for the purpose of public safety, crime prevention and detection
Evidence gathered may be used to prosecute offenders.
This scheme is controlled by Darlington Borough Council
Tel: 01325 405999'

'CCTV 24 hr video recording
Images are being recorded in this area for the purpose of building security, staff and public safety.
Evidence gathered may be used to prosecute offenders.
This scheme is controlled by Darlington Borough Council
Tel: 01325 405999.'

9. BODY WORN CAMERAS

The use of Body Worn CCTV can be beneficial in a number of ways. It can be used to instantly record incidents, act as a visible deterrent to verbal and physical abuse towards officers, provide evidence to support internal or other investigations and strengthen accountability and transparency. The Council's **Body Worn Camera Policy** (see appendix 5) provides users and supervisors with the guidance they require to ensure that the use of Body Worn Cameras complies with the relevant legislation.

10. OWNERSHIP/COPYRIGHT ISSUES

Darlington Borough Council's CCTV schemes are registered under the Data Protection Act 1998. The Data Controller is Darlington Borough Council. All data will be processed in accordance with the stated purpose ensuring compliance with the Act.

CCTV – Primary request to view data

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:

- Providing evidence in criminal proceedings.
- Providing evidence in civil proceedings or tribunals.
- The prevention of crime.
- The investigation and detection of crime (may include identification of offenders).
- Identification of witnesses.

Third parties, who are required to show adequate grounds for disclosure of data within the above criteria, may include, but not limited to:

- Police.
- Statutory authorities with powers to prosecute, (e.g. Customs and Excise, Trading Standards, etc)
- Solicitors.
- Claimants in civil proceedings.
- Accused persons or defendants in criminal proceedings.
- Insurances.
- Other agencies, (as agreed by the Data Controller and notified to the Information Commissioner) according to purpose and legal status.

Upon receipt from a third party of a bona fide request for the release of data, the data controller shall:

- Not unduly obstruct a third-party investigation to verify the existence of relevant data.
- Ensure the retention of data which may be relevant to a request, but which may be pending application for or the issue of a court order or subpoena. A time limit shall be imposed on such retention which will be notified at the time of the request.

Where requests fall outside the terms of disclosure and Subject Access legislation, the data controller or nominated representative shall:

- Be satisfied that there is no connection with any existing data held by the police in connection with the same investigation.
- Treat all such enquires with strict confidentiality.

CCTV – Secondary request to view data

For example, where a member of the public request's CCTV images of their vehicle in a car park where there has been an incident of criminal damage or a fail to stop incident.

By complying with a secondary request, the data controller shall ensure that:

- The request does not contravene, and that compliance with the request would not breach, current relevant legislation, (e.g. Data Protection Act 2018, Human Rights Act 1998, section 163 Criminal Justice and Public Order Act 1994, etc).
- Any legislative requirements have been complied with, (e.g. the requirements of the Data Protection Act 2012), Protection of Freedoms Act 2012.
- Due regard has been taken of any known case law (current or past) which may be relevant, (e.g. R v Brentwood C ex p. Peck).
- The request would pass a test of 'disclosure in the public interest'.

If, in compliance with a secondary request to view data, a decision is taken to release material to a third party, the following safeguards shall be put in place before surrendering the material:

- In respect of the material to be released under the auspices of 'crime prevention', written agreement to the release of the material should be obtained from a police officer, not below the rank of inspector. The officer should have personal knowledge of the circumstances of the crime/s to be prevented and an understanding of the CCTV System Code of Practice.
- If the material is to be released under auspices of 'public wellbeing, health or safety', written agreement to the release of material should be obtained from a senior officer within the Local Authority. The officer should have personal knowledge of the potential benefit to be derived from releasing the material and an understanding of the CCTV System Code of Practice.

Recorded material may be used for bona fide training purposes such as police or staff training. **Under no circumstance** will recorded material be released for commercial sale of material for training or entertainment purposes.

CCTV – Individual Subject Access under Data Protection Legislation

Under the terms of Data Protection legislation, individual access to personal data of which that individual is the data subject must be permitted providing:

- The request is made in writing.

- The data controller is supplied with sufficient information to satisfy him or her self as to the identity of the person making the request.
- The person making the request provides sufficient and accurate information about the time, date and place to enable the data controller to locate the information which that person seeks, (it is recognised that a person making a request is unlikely to know the precise time. Under those circumstances it is suggested that within one hour of accuracy would be a reasonable requirement).
- The person making the request is only shown information relevant to that particular search and which contains personal data of her or himself only unless all other individuals who may be identified from the same information have consented to the disclosure.

In the event of the data controller complying with a request to supply a copy of the data to the subject, only data pertaining to the individual should be copied, (all other personal data which may facilitate the identification of any other person should be concealed or erased).

The data controller is entitled to refuse an individual request to view data under these provisions if insufficient or inaccurate information is provided, however every effort should be made to comply with subject access procedures and each request should be treated on its own merit.

In addition to the principles contained within the Data Protection legislation, the data controller should be satisfied that the data is:

- Not currently and as far as can be reasonably ascertained not likely to become part of a 'live' criminal investigation.
- Not currently and as far as can be reasonably ascertained not likely to become relevant to civil proceedings.
- Not the subject of a complaint or dispute which has not been actioned.
- The original data and that the audit trail has been maintained.
- Not removed or copied without proper authority.
- For individual disclosure only (i.e. to be disclosed to a named subject).

<u>CCTV Retrieval & Point of Transfer (POT) Fees</u>

CCTV requests are chargeable with the exception of law enforcement agencies such as the Police.

Fees:

£120.00 for up to first 4 hours of CCTV footage.
Fee includes labour time, statements, sundries, storage media, secure delivery and all administration.

After the initial 4 hours there will be an hourly rate charge of £30 per hour or part hour to cover officer time. As per DBC's re-use of public sector information policy.

E.g. request for 5hrs 25mins of footage
£120.00 + £60 = £180.00

Payment: (Raising a sundry debtor using Xentrall system)

Requester is required to provide:
Name
Address
Post Code
Ref No.

Copy of CCTV to be retained on record by DBC in accordance with data storage and destruction procedures set out in DBC CCTV Code of Practice.
VAT N/A (Non-business)

CCTV – Procedure for the release of evidence

The Council is committed to the belief that everyone has the right to respect for his or her private and family life. Although the use of CCTV cameras has become widely accepted in the UK as an effective security tool, those people who do express concern tend to do so over the handling of the information (data) which the system gathers.

After considerable research and consultation, a nationally recommended standard has been adopted by the Council.

All requests for the release of data shall be channelled through the data controller or his/her nominated representative.

CCTV – Process of disclosure

Replay the data to the requester only, (or responsible person acting on behalf of the person making the request).

The viewing should take place in a separate viewing booth/room and not in the control or monitoring area. Only data that is specific to the search request shall be shown.

It must not be possible to identify any other individual from the information being shown, (any such information will be blanked-out either by means of electronic screening or manual editing on the monitor screen).

If a copy of the material is requested and there is no on-site means of editing out other personal data, then the material shall be sent to an editing house for processing prior to being sent to the requestee.

For complaints about the use of the Council's CCTV scheme, refer to section 1.

11. CAPTURE, PROTECTION AND STORAGE OF DATA

System operators should adopt the 12 guiding principles under the Home Office's Surveillance Camera Code of Practice.

Because of differences in some of our CCTV systems, image retention periods on systems differ. All new systems and upgraded systems will retain images for 31 days as a maximum period of available for download.

Whichever medium is chosen for the capture and initial storage of images, effective means are made available for transferring the images to the computer system where they are able to be used and possibly archived.

Images on reusable media should be copied from the original storage medium in the original file format onto a secure media. This secure media could be Write Once Read Many (WORM) or secure network storage. The term 'secure server' should be taken to mean an environment, including a security management system, which is accredited to a level of at least 'OFFICIAL' under the Government Classification Scheme (GCS). Once the images and associated data have been copied onto the secure media, they cannot be overwritten or altered.

The generation of the secure copy will be carried out as soon as possible after the capture to reduce the time and opportunity for the accidental or malicious alteration to images.

All imagery master and working copies will be appropriately identified in order to facilitate the storage, retrieval and eventual disposal of case material.

Any downloaded data exhibited in Court as evidence must be the Master Copy. There must be no editing or recording from other sources on to the master copy. However, while the master copy is in Police possession, the Police may take one working copy of the disc and a second copy of the disc to be used as disclosure material to the defence. Written statements will be required from the Police Officers as supporting evidence on copying and other handline of the transferred images onto the disc.

As a rule, unless requested the Council does not keep a copy of the requested CCTV.

The software required for viewing proprietary formats will be made available to avoid images being inaccessible. Replay software will be provided with each recording to assist with the correct viewing of the files in their native format.

Working copies can be in many forms. The files will be copied onto any suitable medium or distributed electronically using a secure system only for circulation to the Investigating officer or Crown prosecution Service.

Those that are retained for evidential purposes must be retained in a secure place to which access is controlled such as a secure safe.

12. CATALOGUING OF DOWNLOADED DISCS

Data downloaded to any storage medium will be given a unique reference number and recorded in the CCTV data request register.

The data will then be stored securely at the CCTV Control Centre in Darlington until collected by the Investigating Officer or representative.

13. ERASURE OF RECORDED IMAGES

Any recording made on the Council's CCTV systems will be automatically overwritten by the server after a set period of time. This will be 30 days.

14. STORAGE/DESTRUCTION OF TRANSFERRED IMAGES

Transferred images will be stored securely to ensure that there is no unauthorised access or possibility of accidental or intentional damage. The storage space should be kept dust and moisture free and kept at a constant temperature and always kept locked when not in use. Only authorised key holders will have access to the secure area. Images removed from the systems actual storage drive which is then deemed to be of no further use or the requester has not collected the images will after advisement safeguards be destroyed after **one further month** and recorded in the CCTV destruction log. Retention of data can no longer be subject to appeals and sentencing for example.

15.USE OF AUDIO

None of Darlington Borough Council's CCTV systems are configured to record any audio activity in conjunction with the video recording accept in the case of private interviews within some Council offices and rooms. Signs are clearly displayed and marked where audio is used.

16. POLICE USE OF RECORDED IMAGES (including Point of Transfer)

When the Police have reasonable cause to believe that an incident has been recorded which involves or may involve criminal activity a duly authorised Police Officer will be handed the downloaded date against signature in accordance with the strict procedures in place.

A 'point of transfer' will be established in which the responsibility of data transfer handling to the Police. That point of transfer will depend on the nature of the image being transferred, the recording format and equipment used by Darlington Borough Council. At whatever stage this point of transfer occurs the Police audit trail must start from that point. Continuity of data handling will be demonstrated throughout, ensuring that the Police audit trail links directly to the Council's audit trail.

The Police have speciality facilities for copying data.

Recorded images owned and managed outside Local Authority Control may require to be processed by copying or the production or reproduction of still images.

The Information Commissioner has approved a process whereby Local Authorities may process data on behalf of a third-party Data Controller for policing purposes.

The process will ensure that the third-party Data Controller, the Data Processor (Local Authority) and the Police will be seen to have made every effort to comply with the seventh principle of data protection law.

At the conclusion of use of any Master or Copy recorded by Police, it may be returned to the Council, unless the Court directs that it should be destroyed instead of being handed back to the owners. In the latter case a certificate of instruction will be provided by the Police to finalise the audit trail relating to those data images.

17. PROVISION OF RECORDED STILLS

The photographic process should only be used to assist in the identification of incidents or in training or for demonstration purposes. Still photographs will not be taken as a matter of routine.

A Police Officer may request the owners to produce still frame images from recordings, also known as snapshots. All such stills will be given a unique reference number and be recorded in the CCTV data request register. All still photographs will remain the property of its owners.

Any still image provided by the Council to the Police will be kept secure and its handling logged in exactly the same way as recorded images. Any stills handed to the Police should be treated on the basis that they are required in Court. The still image is therefore to be placed in a sealed envelope with an exhibit label attached and a Witness Statement provided.

18. DARLINGTON BOROUGH COUNCIL VIEWING OF RECORDED IMAGES

A Council staff member may request to view the recording of a specified incident which does not involve or appear to involve criminal activity but which may involve the management services for which the officer is responsible (i.e. Housing, Parking) if the officer has been made aware of an incident through other means and has reason to believe the CCTV may assist them.

- Any private viewings must be first approved by the Data Protection Officer
- A log will be kept of any such viewings
- No other viewings by an unauthorised person will be permitted

19. EVALUATION, MONITORING AND AUDIT OF SCHEME

The scheme owners should arrange for independent evaluation to establish whether the purposes as stated are receiving compliance and whether the objectives are being achieved.

The process should include:

a) Assessment of the impact on crime the system has had
b) Assessment and comparison of neighbouring areas without CCTV
c) Views of the public
d) Operation of the Code of Practice
e) Whether the purposes and key objectives of the system remain valid
f) Complaints received relating to the use of the scheme
g) Data Protection and legal requirements
h) Maintenance schedule and performance test of the systems

Evaluation should be provided for in annual budgetary considerations.

An Annual Report may be compiled and made available for public information by the Council, or their advisers. The topics covered within the report should include details of the following:

a) A description of the scheme and the geographical areas of operation
b) The scheme's policy statement
c) The purpose and scope of the 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 scheme
g) The aims and objectives for the next 12 months (CCTV Strategy)

Any Annual Report will also provide details of the schemes' achievements during the previous 12 months, which may be based on information already held by the scheme. The assessment of the schemes' performance should include:

a) The number of incidents recorded by the scheme
b) The number of incidents reported to the Police ad, where appropriate, other bodies, e.g. the local authority
c) An assessment of the CCTV scheme's impact on crime levels and types of crime in the area covered by the scheme