Southampton City Council

Closed Circuit Television (CCTV) Policy

2020

SOUTHAMPTON
CITY COUNCIL

Southampton City Council
CCTV Policy
2020

Contents

CCTV Policy			
Version	6	**Approved by**	Information Governance Board
Date last amended	May 2020	**Approval date**	9th September 2020
Lead officer	Chris Thornton, Information Lawyer (Data Protection Officer)	**Review date**	9th September 2021
Contact	dataprotection@southampton.gov.uk	**Effective date**	24th September 2021

1. Purpose

1.1 The aim of this policy is to help employees operating Closed Circuit Television (CCTV) schemes or other forms of surveillance cameras or surveillance systems on behalf of Southampton City Council to do so in full compliance of the Data Protection Act 2018 and General Data Protection Regulation (EU) 2016/679, Human Rights Act 1998, Regulation of Investigatory Powers Act 2000 (RIPA), Protection of Freedoms Act 2012 and in adherence to high standards of good practice as laid out by the Information Commissioner's Office.

1.2 Public authorities and those organisations carrying out the functions of a public service nature are required to observe the obligations imposed by the Human Rights Act 1998.

1.3 Section 163 of the Criminal Justice and Public Order Act 1994 creates the power for local authorities to provide CCTV coverage of any land within their area for the purposes of crime prevention or victim welfare and it is also considered a necessary initiative by Southampton City Council towards their duties under the Crime and Disorder Act 1998.

1.4 It is recognised that the operation of a surveillance camera system may be considered to infringe on the privacy of individuals. The Council recognises that it is its responsibility to ensure that a surveillance camera system should always comply with all relevant legislation, to ensure its legality and legitimacy. A surveillance camera system will only be used as a proportional response to identified problems and be used only in so far as it is necessary in democratic society, in the interests of national security, public safety, the economic well being of the area, for the prevention and detection of crime or disorder, for the protection of health and morals, or for the protection of the rights and freedoms of others.

1.5 This policy should be read in conjunction with the latest guidance from the Information Commissioner's Office, the Surveillance Camera Code of Practice issued by the Secretary of State, and Southampton City Council's Information Governance policies.

2. Scope

2.1 This policy applies to all CCTV and related surveillance systems operated by Southampton City Council .

2.2 Southampton City Council, as the Data Controller, has determined the purposes for which any personal data are, or are to be, processed as follows:

- To help reduce the fear of crime to provide a safe and secure environment for residents of, and visitors to, the areas covered by the scheme.
- The help deter and detect crime and provide evidential material for court proceedings.
- To assist in the overall management of Southampton City Council.
- To assist in the management of Southampton City Council's Housing Stock covered by the Concierge Service.
- To assist in the management of other locations and buildings owned or controlled by Southampton City Council.
- To enhance community safety, including the prevention and detection of harassment, to assist in developing the economic well-being of the Southampton area and encourage greater use of the city centre.

- To assist the local authority in their enforcement and regulatory functions within the Southampton area.
- To assist in traffic management, and encourage safer and more sustainable use of all modes of transport and provide travel information to the media and public.
- To assist in supporting civil proceedings.
- To identify breaches of tenancy terms and to supply evidence to support enforcement action, this may include civil proceedings.
- To monitor all modes of travel to enable improvement and better management of the public highway (traffic cameras).
- To assist the Council discharge its health and safety obligations towards staff

3. Definitions

3.1 CCTV – Closed Circuit television (CCTV) is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors.

3.2 Data means information which –

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,

(b) is recorded with the intention that it should be processed by means of such equipment,

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or

(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d) above.

3.3 Data controller – means … a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

3.4 Data subject means an individual who is the subject of personal data.

3.5 Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

3.6 ICO – The Information Commissioner's Office (ICO) is the UK's independent body set up to uphold information rights.

3.7 Personal data means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

3.8 DPIA –Dara Protection Impact Assessments are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.

3.9 Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3.10 Surveillance system - this policy applies to those involved in operating CCTV and other surveillance camera devices that view or record individuals, and covers other information that relates to individuals, for example vehicle registration marks captured by ANPR equipment. This policy uses the terms 'surveillance system(s)', 'CCTV' and 'information' throughout for ease of reference.

4. Policy statement

4.1 Setting up a surveillance system

4.1.1 A Data Protection Impact Assessment (DPIA) MUST be undertaken at the outset before any new proposal for a surveillance system is agreed in accordance with the Council's guidance on DPIAs [intranet link]. All privacy risks of the proposal must be identified and managed and only when the Data Protection Officer, or his appointed delegate has confirmed that your proposed measures are adequate and has approved your proposal, can you proceed. The DPIA should be kept under regular review whilst the system is operational.

4.1.2 The use of the surveillance system must take into account the nature of the problem you are seeking to address; whether a surveillance system would be a justified and effective solution and whether better solutions exist

4.1.3 Use of a surveillance camera system be proportionate and must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

4.1.4 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.

4.1.5 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.

4.1.6 There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

4.1.7 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.

4.1.8 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.

4.1.9 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.

4.1.10 Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

4.1.11 Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

4.1.12 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.

4.1.13 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.

4.1.14 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.

4.1.15 Any approved surveillance cameras not covered by the Council's existing notification will be notified to the Information Commissioner's Office.

4.2 Operation of surveillance systems

4.2.1 Southampton City Council will operate the surveillance system in accordance with the guidance published by the Information Commissioner's Office, the Surveillance Camera Code of Practice and Southampton City Council's Information Governance policies. The ICO guidance includes guidance as to how systems are selected and sited, who they are to be operated by and how personal information is to be stored and retained. The Codes, guidance and policies MUST be complied with by the Managers responsible for the services which utilise surveillance systems and Managers will ensure compliance by all members of their staff

4.2.2 All who use surveillance systems on behalf of Southampton City Council will also act in accordance with the Operational Procedures at Appendix A and sign the Declaration at Appendix B.

4.3 Requests to access information

4.3.1 Requests for the release of data are to be passed to the Corporate Legal Team. The Data Protection Officer (on behalf of the Council) can refuse an individual request to view footage, if insufficient or inaccurate information is provided. A search request should specify reasonable accuracy i.e. within 30 minutes.

4.3.2 Details are included at Appendix C or online at: http://www.southampton.gov.uk/council-democracy/council-data/data-protection/request-cctv-footage.aspx

4.4 Subject Access Requests / Requests to view data for evidential purposes

4.4.1 These will be handled in accordance with Southampton City Council's Information Access and Use: Access to Personal Records Policy.

4.5 Police requests for CCTV information

4.5.1 Requests from Hampshire Constabulary will be handled in accordance with the joint Hampshire Constabulary/Southampton City Council "Protocol for Police Access to CCTV Footage".

4.6 Complaints Procedure

4.6.1 Complaints about the Council's surveillance camera systems should be directed to the Senior Responsible Officer for Surveillance Systems, who can be contacted at:

dataprotection@southampton.gov.uk.

4.6.2 In a complaint, please give us as much information as you can, including:

- what went wrong
- when it happened
- who you have dealt with so far
- how you would like the matter resolved

5. Management

5.1 The Council's Information Governance Board have oversight of this Policy, and the Council's Data Protection Officer has been identified as its CCTV Senior Responsible Officer for Surveillance Systems (SRO), who will have strategic responsibility for the integrity and efficacy of the processes in place within the Council that ensure compliance with the Protection of Freedoms Act 2012, and in respect of all surveillance camera systems operated by the Council.

5.2 The SRO is supported by single points of contact (SPOCs) who are officers who administer the CCTV systems at an operational level. The SRO and the SPOCs will work together to ensure this policy is implemented across Southampton City Council services, and will meet on a regular basis as a CCTV User Group. The SRO can act as the first point of contact for the work of this group (dataprotection@southampton.gov.uk).

5.3 The SPOCs will monitor implementation and compliance with this policy for the systems they administer. Users found in breach of this policy may be subject to disciplinary action.

6. Governance

6.1 The Corporate Legal Team oversees this policy.

6.2 The CCTV user-group is responsible for implementing this policy.

6.3 The Information Governance Board is accountable for this policy.

OPERATIONAL PROCEDURES

Introduction

These Operational Procedures have been drawn up in conjunction with the CCTV Code of Practice 'the Code' and the guidance from the Information Commissioner's Office which sets out minimum standards expected of all employees and authorised users managing and operating the System. The efficient and legal operation of CCTV rests with the standards contained within the Code. It should be considered as a benchmark for good practice that will ensure accountability and command employee and public confidence.
The Code will be the principal document for the resolution of any difficulties or discrepancies that may arise from the operation of the System.
The Code together with these Operational Procedures will be subject to amendments and updates as required. It is the responsibility of all staff working with the System to ensure that at all times they adhere to the contents of these documents. The documents have been written against the legal requirements of the Human Rights Act 1998. It is incumbent upon all staff to draw to the attention of the Data Controller any departure from the terms of the Code or its related Operational Procedures.

a. Operator duties and responsibilities
The very nature of CCTV is that it poses an intrusive breach of an individual's privacy. The majority of those who visit or pass by cameras will do so without an understanding of the range and capability of the cameras. The parties recognise the very real position and trust that those who operate the System have. In recognising the legal requirements of the Human Rights Act 1998, Data Protection Act 2018 and General Data Protection Regulation (EU) 2016/679, and the Regulation of Investigatory Powers Act 2000, the parties have sought to provide those who operate the System with clear guidance on their duties and responsibilities.

b. Purposes of the System
The System must not be used for any purpose other than those defined in the policy (see section 2 of the policy). Any failure to follow the Code will result in disciplinary action being taken against members of staff. In the context of the defined purposes of the System the cameras can be used in the detection of criminal activity as well as for the safety of people visiting and working in the area immediately covered by the camera.

c. System integrity
The CCTV Operators should have regard for the safety and well being of those using the areas covered by the cameras. In particular the individual's right to privacy must not be unduly infringed. To this end all Operators are required to:
Sign a Declaration of Confidentiality that will remain in force throughout their period of employment;

Undergo a period of training on the operation of the System and its related procedures;
Know the contents of the Code and these Operating Procedures;
Be aware at all times of the potential abuse there may be in operating the System;
e.g. looking into private areas such as office windows or people in their vehicles, unless such actions are justified through prior information;
Attend court as required to support evidence that might have been gathered in the course of their duties.

d. Selection and recruitment

Each Operator will be subject to appropriate background checks and will be expected to demonstrate their understanding and commitment to total confidentiality at all times.

e. Training

The training required by a CCTV Operator will include company related information as well as technical and legal information. Operators will be provided with training in using the System. They will be encouraged to undertake further training to industry recognised standards. As such the Operators must know: The technical operation of the System including any training given by the equipment manufacturers and installers;
How to interpret the Code and relation Operational Procedures;
The geographical location and coverage of every camera in the System;
The legal issues surrounding privacy and potential contravention of the Human Rights Act 1998, Data Protection Act 2018 and General Data Protection Regulation (EU) 2016/679, and the Regulation of Investigatory Powers Act 2000.

f. Discipline

CCTV Operators will be subject to relevant discipline codes. Any breach of these Operational Procedures, the Code or confidentiality will be dealt with in accordance with those discipline regulations and staff must recognise that any such breach may amount to gross misconduct, which could lead to dismissal.
All parties will accept prime responsibility for ensuring that there is no breach of security and that the Code and Operational Procedures are complied with. Those having day-to-day responsibility for the management of the Control Room will also have responsibility for enforcing the discipline regulations.

Appendix B

DECLARATION

I_____ (name) undertake duties that include the use of surveillance systems on behalf of Southampton City Council. I have received a copy of the Southampton City Council CCTV Code of Practice and guidance from the Information Commissioner's Office, the Surveillance Camera Code of Practice issued by the Secretary of State, and Southampton City Council's Information Governance policies.

I hereby declare that:

I am fully conversant with the content of the Code and guidance and understand that all the duties which I undertake in connection with surveillance systems must not contravene any part of the Code, or any future amendments of which I am aware.

If now, or in the future, I am or become unclear of any aspect of the operation of the surveillance systems or the content of the Code/guidance, I undertake to seek clarification of any such uncertainties.

I understand that it is a condition of my employment that I do not disclose or divulge to any individual, firm, company, authority, agency or other organisation, any information which I may have acquired in the course of, or for the purposes of, my position in connection with the surveillance systems, verbally, in writing or by any other media, now or in the future.

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

Signed:_____

Print name:_____

Witness:_____

Position:_____

Dated this_____ day of _____ (month) 20_____

Appendix C

REQUEST CCTV INFORMATION

http://www.southampton.gov.uk/council-democracy/council-data/data-protection/request-cctv-footage.aspx

If you have been involved in an incident, and wish to view the CCTV footage, please follow the steps below in order to make your request:

1. Act now. CCTV footage is only held for 31 days, so please inform us as soon as possible if you need this footage to be saved for evidential purposes.

2. Locate the camera. Please check our interactive map to find details of every CCTV and Traffic camera in the city. This will help you identify the camera(s) which may have caught the incident.

3. Provide details of the incident. Complete our CCTV footage request form. Please provide us with detailed information, such as location, time (to within 30 minutes), and vehicle details. This will enable us to locate and save the footage most relevant to you. Once secured, we will provide you with a reference number for the footage.

Important information

If you are not the only person in the footage, we will only release CCTV footage to you directly if we don't have any privacy concerns.

These concerns will be because one or more of the following apply:

- The length of footage is too long, meaning that the amount of personal information captured is too great. **Generally, requests for footage should be limited to half an hour**
- There is a high likelihood of individuals being identified
- The risk of prejudice to those individuals if re-identification occurs is high
- The individuals in the footage have a higher expectation of privacy due to the location of the camera
- The incident captured is of a sensitive nature (e.g. a criminal offence or road traffic accident)

If there are other people in the footage and we have privacy concerns, we will not be able to release the footage to you directly.

If we cannot release the footage to you directly, the Police or your insurance company have powers to request this information on your behalf, and we may be able to release it to them instead.

Please note, however, that if an organisation (other than the police) makes a request for CCTV footage, a non-refundable fee of £50.00 may be payable. Please see our Access to Information Charging Policy (pdf) for further details.

For further information you can email information@southampton.gov.uk