CCTV
and Surveillance Camera Policy

Policy Details

Version
7.1
Approved by
Information Governance Board
Lead officer
Information Lawyer (Data Protection Officer)
Contact
dataprotection@southampton.gov.uk
Date last amended
19th January 2022
Approval date
19th January 2022
Effective date
19th January 2022
Review date
19th January 2023

Contents

1. Policy Summary

1.1. Southampton City Council (the Council) has in place Closed-Circuit Television (CCTV) and other surveillance systems. This policy details the purpose, use, and management of the systems, and details the procedures to be followed in order to ensure that the Council complies with relevant legislation and Codes of Practice where necessary.

1.2. This policy and the procedures therein detailed, applies to all of the Council's CCTV and surveillance systems, including overt and covert installations capturing images of identifiable individuals for the purpose of viewing, and / or recording the activities of such individuals.

1.3. CCTV and surveillance system images are monitored and recorded in strict accordance with this policy.

2. Introduction

2.1. The Council uses CCTV and surveillance system images for the prevention and detection of crime, public safety, to monitor the Council's buildings in order to provide a safe and secure environment for staff, volunteers, contractors, and visitors, and to prevent the loss of or damage to the Council's contents and property.

2.2. The CCTV and surveillance systems are owned by the Council and managed by the Council and / or its appointed agents. The Council is the system operator, and data controller, for the images produced by the CCTV and surveillance systems, and is registered with the Information Commissioner's Office, Registration number Z4809838.

2.3. This policy applies to 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.

2.4. This policy uses the terms 'surveillance system(s)', 'CCTV' and 'information' throughout for ease of reference, and would include (but is not limited to) the following types of systems:

2.4.1. Fixed CCTV (networked)
2.4.2. Body Worn Video
2.4.3. ANPR
2.4.4. Unmanned aerial systems (drones)
2.4.5. Stand-alone cameras
2.4.6. Redeployable CCTV

3. Purpose

3.1. This Policy governs the installation and operation of all CCTV and surveillance systems at the Council.

3.2. CCTV surveillance is used to monitor and collect visual images for the purposes of:

- 3.2.1. 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.
- 3.2.2. The help deter and detect crime and provide evidential material for court proceedings.
- 3.2.3. To assist in the overall management of the Council.
- 3.2.4. To assist in the management of the Council's housing stock.
- 3.2.5. To assist in the management of other locations and buildings owned or controlled by the Council.
- 3.2.6. 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.
- 3.2.7. To assist the local authority in their enforcement and regulatory functions within the Southampton area.
- 3.2.8. 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.
- 3.2.9. To assist in supporting civil proceedings.
- 3.2.10. To identify breaches of tenancy terms and to supply evidence to support enforcement action, this may include civil proceedings.
- 3.2.11. To monitor all modes of travel to enable improvement and better management of the public highway (traffic cameras).
- 3.2.12. To assist the Council in discharging its health and safety obligations towards staff
- 3.2.13. To investigate allegations of staff misconduct

4. Scope

4.1. This policy applies to all CCTV and related surveillance systems operated by the Council.

4.2. Where a system is jointly owned or jointly operated, the governance and accountability arrangements are agreed between the partners and documented so that each of the partner organisations has clear responsibilities, with clarity over obligations and expectations and procedures for the resolution of any differences between the parties or changes of circumstance.

4.3. This policy is applicable to, and must be followed by, all staff including consultants and contractors. Failure to comply could result in disciplinary action, including dismissal. This policy also applies to volunteers and Council Members.

4.4. All staff involved in the operation of the CCTV System will be made aware of this policy and will only be authorised to use the CCTV System in a way that is consistent with the purposes and procedures contained therein.

4.5. All systems users with responsibility for accessing, recording, disclosing or otherwise processing CCTV images will have relevant skills and training on the operational, technical and privacy considerations, and fully understand the policies and procedures.

5. Policy Statement

5.1. The Council will operate its CCTV systems in a manner that is consistent with respect for the individual's privacy.

5.2. The Council complies with the Information Commissioner's Office (ICO) CCTV Code of Practice and the Surveillance Camera Commissioner's Surveillance Code of Practice to ensure CCTV is used responsibly and safeguards both trust and confidence in its continued use.

5.3. The CCTV systems will be used to observe the areas under surveillance in order to identify incidents requiring a response. Any response should be proportionate to the incident being witnessed.

5.4. The use of the CCTV systems will be conducted in a professional, ethical, and legal manner, and any diversion of the use of CCTV security technologies for other purposes is prohibited by this policy.

5.5. Cameras will be sited so they only capture images relevant to the purposes for which they are installed. In addition, equipment must be carefully positioned to:

5.5.1. cover the specific area to be monitored only;
5.5.2. keep privacy intrusion to a minimum;
5.5.3. ensure that recordings are fit for purpose and not in any way obstructed (e.g. by foliage);
5.5.4. minimise risk of damage or theft

5.6. Before any CCTV system is installed, service areas will consider other, less intrusive methods to achieve the objectives of having a CCTV system in place (e.g. improving lighting in an area to prevent crime).

6. Location and signage

6.1. Cameras are sited to ensure that they cover the relevant areas as far as is possible. Cameras are installed throughout the site/s including roadways, car parks, buildings, premises, within buildings and vehicles, and externally in public facing areas.

6.2. The location of equipment is carefully considered to ensure that images captured comply with data protection requirements. Every effort is made to position cameras so that their coverage is restricted to the relevant area, which may include outdoor public spaces.

6.3. Signs are placed wherever CCTV systems are in operation, in order to inform individuals that CCTV is in operation.

6.4. The signage indicates that monitoring and recording is taking place, for what purposes, who the system owner is (if it is not obvious), and where complaints / questions about the systems should be directed.

6.5. An example sign is below:

7. Monitoring and Recording

7.1. Cameras are monitored in a secure private offices and locations.

7.2. System administrators can view and access footage for the purposes for which the CCTV system is in operation. Before any further disclosure is made (e.g. to an external organisation, or another internal department / member of staff), advice should be sought from the Corporate Legal team.

7.3. Images are recorded on secure servers (ideally standalone systems, not connected to the network) and are viewable by the system administrators. Additional staff may be authorised by the system administrator to access images from cameras sited within their own areas of responsibility.

7.4. Any staff who has access to the system are made aware of their roles and responsibilities relating to the system by the system administrator, who will also provide them with the necessary skills and knowledge to use and manage the system.

7.5. Staff who have access to the system will receive continued training as needed, to ensure their competence relating to relevant operational, technical, privacy considerations, policies and procedures.

7.6. Where service areas are using Cloud-based storage, they will ensure that such storage is located in the UK or European Economic Area (EEA), and that all relevant security and data protection measures are in place.

7.7. Recorded material will be stored in a way that maintains the integrity of the image and information to ensure that metadata (e.g. time, date and location) is recorded reliably, and compression of data does not reduce its quality.

7.8. Viewing monitors should be password protected and switched off / lock when not in use to prevent unauthorised use or viewing.

7.9. The cameras installed provide images that are of suitable quality for the specified purposes for which they are installed, and all cameras are checked regularly to ensure that the images remain fit for purpose, and that the date and time stamp recorded on the images is accurate.

8. Covert Surveillance

8.1. Covert surveillance is the use of hidden cameras or equipment to observe and / or record the activities of a subject which is carried out without their knowledge.

8.2. The use of covert cameras or recording / monitoring will be restricted to rare occasions, in accordance with the Council's RIPA Corporate Surveillance Guidance[1].

9. Employee Monitoring

9.1. Any use of Council CCTV systems to monitor staff (either overtly or covertly) must be done so in accordance with the Council's Employee Monitoring Policy[2].

9.2. The use of CCTV images to monitor staff must be approved by the Council's Senior Information Risk Owner (SIRO).

10. Data Protection Impact Assessments

10.1. In its administration of its CCTV systems, the Council complies with the General Data Protection Regulation (UK GDPR). the Data Protection Act 2018, and in accordance with its own Data Protection Policy[3].

10.2. The Council's CCTV systems (new and existing) are subject to a Data Protection Impact Assessment (DPIA)[4], identifying risks related to the installation and use of the system, ensuring full compliance with the data protection principles. This will include consultation with relevant internal and external stakeholders.

10.3. Once systems are operational, system administrators will conduct regular reviews of the DPIA for their system.

11. Subject Access Requests

11.1. Requests by individual data subjects for images relating to themselves via a Subject Access Request should be submitted to the Corporate Legal team at information@southampton.gov.uk. Further details of this process are detailed in the Council's Access to Personal Records Policy[5], or the Council's website[6].

11.2. In order to locate the images on the system, sufficient detail must be provided by the data subject in order to allow the relevant images to be located and the data subject to be identified.

---

[1] https://staffinfo.southampton.gov.uk/information-governance/policies-and-guidance/default.aspx
[2] https://staffinfo.southampton.gov.uk/information-governance/policies-and-guidance/default.aspx
[3] https://staffinfo.southampton.gov.uk/information-governance/policies-and-guidance/default.aspx
[4] https://staffinfo.southampton.gov.uk/information-governance/data-protection/data-protection-impact-assessment.aspx
[5] https://staffinfo.southampton.gov.uk/information-governance/policies-and-guidance/default.aspx
[6] https://www.southampton.gov.uk/council-democracy/council-data/data-protection/request-cctv-footage

11.3. Where the Council is unable to comply with a Subject Access Request without disclosing the personal data of another individual who is identified or identifiable from that information, it is not obliged to comply with the request unless satisfied that the individual has provided their express consent to the disclosure, or if it is reasonable, having regard to the circumstances, to comply without the consent of the individual.

11.4. A search request should specify reasonable accuracy i.e. within 30 minutes.

11.5. A request for images made by a third party should be made to the Corporate Legal team at information@southampton.gov.uk. Further details of this process are detailed in the Council's Information Sharing Policy[7], or the Council's website[8]

12. Third Party Disclosures

12.1. In limited circumstances it may be appropriate to disclose images to a third party, such as when a disclosure is required by law, in relation to the prevention or detection of crime or in other circumstances where an exemption applies under relevant legislation.

12.2. Such disclosures will be made at the discretion of the system administrator, with reference to relevant legislation, and following advice from the Corporate Legal team.

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

12.4. A log of any disclosure made under this policy will be held by the relevant system administrator. The log should include (at a minimum) the date that a disclosure was made, the recipient, and the reason for disclosure.

12.5. Before disclosing any footage, consideration should be given to whether (if possible) images of third parties should be obscured to prevent unnecessary disclosure.

12.6. Where information is disclosed, the disclosing officer must ensure information is transferred securely, and the following instructions on the use of the images given to the recipient:

[7] https://staffinfo.southampton.gov.uk/information-governance/policies-and-guidance/default.aspx
[8] https://www.southampton.gov.uk/council-democracy/council-data/data-protection/info-about-others/

"Once Southampton City Council has disclosed this footage to you, you become the data controller for the copy held by you. It is your responsibility to comply with data protection legislation in relation to any further disclosures or processing. Representations from Southampton City Council should be sought before further disclosure is made"

13. Retention

13.1. Unless required for evidentiary purposes, the investigation of an offence, or as required by law, CCTV images will be retained for no longer than 31 calendar days from the date of recording (or for certain systems, until storage limitations require that footage needs to be overwritten). Images will be automatically overwritten or destroyed after this time.

13.2. Any footage downloaded and retained for evidential purposes must be reviewed after three months by the system administrator, and either a destruction date or review date must be set, with written justification for further retention recorded.

13.3. CCTV disclosure logs should be kept for 6 years.

14. Complaints Procedure

14.1. Complaints concerning the Council's use of its CCTV systems or the disclosure of CCTV images should be made in the first instance to the service area controlling the system. The contact details should be found on the signage for the relevant system.

14.2. For complaints where contact details can't be identified, these should be made to the Council's Data Protection Officer (dataprotection@southampton.gov.uk).

14.3. Depending on the nature of the complaint, it will either be processed under the Council's Corporate Complaints process, or (more likely) treated as a data protection concern to be investigated by the Council's Data Protection Officer.

15. Management

15.1. The Council's Information Governance Board has oversight of this policy, and the Council's Data Protection Officer has been identified as its CCTV Senior Responsible Officer for Surveillance Systems (SRO).

15.2. The SRO has 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.

15.3. 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).

15.4. 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.