Brighton & Hove City Council

Surveillance Camera Policy

Contents

1. Introduction

This policy governs the operation of surveillance camera technology (including closed circuit television (CCTV) systems and other overt surveillance technology) operated by Brighton & Hove City Council as a data controller to assist it in carrying out its enforcement, public safety, and other functions.

The policy sets out the principles to be observed by the Council, its members, employees, contractors, and any other parties or organisations involved in the operation, management, and administration of relevant surveillance camera systems, as well as the responsibilities which exist to ensure that these systems are operated in a compliant manner. It is also intended to inform members of the public of the purposes for which cameras are operated, and of the standards to be met in relation to them.

The policy is not binding on Local Authority schools, which are legally distinct from the Council and are separately responsible for any surveillance cameras they may use.

A list of key definitions and acronyms is set out at section 12 of this policy.
This policy does not govern the Council's use of the surveillance powers available to it, which are conducted under the auspices of the Regulation of Investigatory Powers Act. Covert surveillance is governed by a separate document, the RIPA Policy (Corporate Policy & Procedures Document on the Regulation of Investigatory Powers Act 2000).

2. Purpose

Compliance with this policy and with the detailed arrangements which sit under it ensures that the Council's use of surveillance cameras reflects a proportionate response to identified problems, which is operated with due regard to the privacy rights of individuals.

This policy describes and addresses BHCCs obligations regarding the monitoring of public spaces and Council property and the associated use of surveillance camera technology.

This policy exists to:

- ensure compliance with relevant law and codes of practice
- safeguard personal data collected and stored by the council
- ensure consistency and transparency in the Councils use of surveillance camera technology

The Policy is based on adherence to the twelve guiding principles detailed in the Surveillance Camera Code of Practice

3. Background and context

Article 8 of the Human Rights Convention recognises the right to a private and family life. Where surveillance cameras capture images of people which comprise personal data, there is potential for this to infringe on the privacy of individuals. Accordingly, there is an

obligation for surveillance camera installations and handling practices to comply with data protection legislation. Surveillance camera systems are operated by the Council and its partners only as a proportionate response to identified problems where there is a legal basis to do so.

The Information Commissioner's Office ('the ICO') has enforcement powers which include the power to issue directives to remove or modify surveillance camera installations. The ICO is supported by the Biometrics and Surveillance Camera Commissioner that was established under the Protection of Freedoms Act 2012. The Biometrics and Surveillance Camera Commissioner has issued a Code of Practice for the use of surveillance camera technology, which has the status of statutory guidance and which this policy has taken into account.

This policy applies only to the deployment of surveillance camera technology where the Council is the Data Controller and determines the way the technology is to be deployed and use to be made of the footage to be captured. The Council is not responsible for any cameras deployed by other individuals or organisations in or around Council-owned properties which are leased or otherwise made available to other people or bodies under some other arrangement (this includes any subcontractor who deploys the use of surveillance cameras where they are the data controller for footage captured).The Council normally refuses to authorise the installation of surveillance cameras by individuals on Council property e.g. where it holds the freehold, street assets etc.

4. Surveillance cameras within the scope of this policy

The Council acts as data controller for the surveillance camera systems it operates for the purposes of preventing and detecting crime and for ensuring public and staff safety, including that of attendees at its public venues and residents of its social housing.

The Council's City Clean vehicles also have cameras for the purposes of providing evidence for insurance claims.

ANPR cameras are deployed in some bus lanes for enforcement purposes as part of a partnership arrangement with the Police.

Some staff or contractors with public enforcement roles wear body-mounted cameras to protect their safety and wellbeing whilst carrying out their duties. At the time of writing, the Council does not employ the use of drones, however their deployment would also be covered by this policy.

5. General Principles / Guidelines

The Council's use of surveillance camera technology accords with the requirements and the principles of the Human Rights Act 1998, the UK General Data Protection Regulation, the Data Protection Act 2018, and the Protection of Freedoms Act 2012. Surveillance cameras

shall be operated with due regard to the principle that everyone has the right to respect for his or her private and family life and home. Public interest in the operation of surveillance cameras will be recognised by ensuring the security and integrity of operational procedures which sit underneath it, and which balance the objectives of the camera usage with the need to safeguard the individual's rights. The Council will operate all surveillance camera implementations in line with the principles set out in the Surveillance Camera Commissioner Code of Practice.

In order to ensure the Council upholds individuals' rights in processing personal data and complies with relevant legislation, any deployment of the use of surveillance technology must be designed and risk assessed using the following process:

a. A Data Protection Impact Assessment and Surveillance Checklist (see Appendix 1) must be completed and signed off for each use and deployment* of surveillance technology.

b. A technical Risk Assessment must be completed and signed off for each use and deployment of surveillance technology

**Deployment refers to a common instance of Surveillance Camera Technology i.e., using the same technology and processes for the same purpose and can therefore cover more than one camera.*

6. Data Sharing requests

The police, social services, environmental health and/or other authorised agencies or bodies may apply for access to data collected via surveillance cameras in order to carry out their statutory functions. All requests will be reviewed by the Council's data protection team and determined according to a process which ensures compliance with the law.

7. Cameras and Area Coverage

The use of cameras and the positions they are placed in are reviewed annually by relevant services to ensure that they remain proportionate to their purpose. Where the purpose can no longer be justified against the intrusion on personal privacy, they will be removed or switched off.

Where equipment is in use it must be accompanied by clear signage in order or the public to be aware.

Most of the surveillance camera systems do not record audio. Where audio is recorded this is made clear to the public through signage, or where applicable, verbally.

All viewing and recording equipment shall only be operated by trained and authorised users.

8. Roles and Responsibilities

All staff with operational access to surveillance camera equipment are responsible for following the specific operational procedures established for its use. This includes checking the equipment and reporting to management where it is found to deviate from the agreed specification or appears to have been interfered with.

Staff contractors and other relevant persons shall only be permitted access to images obtained via surveillance cameras on a ‘need to know’ basis.

Information Asset Owners are accountable for identifying a legitimate need for surveillance camera installations where this exists (and for reviewing the same), for ensuring that data protection impact assessments are conducted, and an action plan generated and progressed and for making sure that risk controls are established where needed to protect personal privacy.

The Senior Information Risk Owner (SIRO) is the responsible officer for surveillance camera installations for the council. Where any proposed installations are assessed as posing a high risk to personal privacy, these must be reviewed by the Senior Information Risk Owner.

The Data Protection Officer (DPO) is responsible for assessing proposed surveillance camera installations posing a high risk to privacy, rights, and freedoms and for making recommendations to the SIRO. In cases of a serious breach involving surveillance camera data, the DPO is responsible for reporting the matter to the ICO.

The Information Governance Team is responsible for assisting departments with Data Protection Impact Assessments and participating in the investigation of breaches.

9. Data Protection and subject access rights

Individuals whose personal data has been collected via the use of surveillance technology have a right to access and/or obtain a copy of this data and to exercise any other relevant right under Data Protection Law (unless an exemption applies).

To exercise data subject rights (for example, the right of access, erasure, and rectification) individuals can make requests via Information Rights Team. Examples of exercising some of these rights include:

A right to request through subject access, a copy of footage in which they are captured, subject to exemptions within the Data Protection Act 2018 and also balanced against the rights and freedoms of others who may appear in that footage.

A right to object to processing where they believe that the field of vision or the siting of the camera is disproportionate to the stated purpose of the camera. Where a resident objects to processing, the Council will consider the objection and decide whether a lawful basis for processing can still be justified. A written response will be provided outlining the outcome.

10. Data Retention & sharing

Council surveillance cameras are usually set to automatically over-write footage between 28 and 31 days after it is captured. Where authorised bodies are granted access to data collected via surveillance cameras in order to carry out their statutory functions, then copies of the data may be made and provided securely for this purpose.

11. Key Definitions

CCTV – Closed Circuit Television

Data Protection Officer (DPO) – A statutory role set out under data protection legislation with responsibility for ensuring that organisations are compliant with personal privacy rights. Any resident can report a personal privacy concern about the Council to the Data Protection Officer.

UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 - legislation that covers data protection principles and privacy rights.

Information Asset Owner – A role held by senior managers at the Council, to ensure that information systems operated by their teams have appropriate data quality, auditability, and access controls.

Information Governance – The discipline of applying controls to how information or data is created, how it is stored and where it moves.

Senior Information Risk Owner (SIRO) – A role established under International Information Security Standard ISO27001 to ensure that appropriate processes for information risk and the treatment of that risk are established and maintained.

Senior Responsible Officer (SRO) - senior manager who has strategic oversight for the integrity and efficacy of the processes in place within the local authority which ensure compliance with s.33 of PoFA in support of the Chief Executive, and in respect of all relevant surveillance camera systems operated by the local authority.

Surveillance Camera Technology - has the meaning given by Section 29(6) of Protections of Freedoms Act 2012 and includes: closed circuit television (CCTV), automatic number plate recognition (ANPR) systems and any other systems for recording or viewing visual images for surveillance purposes.

RIPA – The Regulation of Investigatory Powers Act 2000. This act sets out the conditions under which investigations and covert surveillance can be lawfully conducted.

12. Review of this Policy

This policy will be reviewed annually under the oversight of the Senior Information Risk Owner.

13. Related Policies

☐ Data Protection Policy
☐ RIPA Policy

14. References

☐ Surveillance Camera Commissioner Code of Practice
☐ Surveillance Camera Self-Assessment Tool

15. Policy Control Details

Policy Name	Surveillance camera policy
Document Type	Internal and External facing policy
Version	2
Introduction date	3 April 2023
Effective date	3 April 2023
Next review date	April 2024
Reviewed by	Heidi Judd, Chris Mitchell
Approved by	Executive Leadership Team
Document author	Heidi Judd
Document Owner	Information Governance Team

Appendix 1: Surveillance Checklist

Privacy Impact

- Is there a clear and legitimate purpose for use of surveillance? E.g., detection and prevention of crime, public safety etc.
- Are there no alternatives to use of surveillance? Is there a pressing need for the use of surveillance technology?
- Is the processing lawful? (Does an applicable condition to process apply?)
- Has the effect on individuals and their privacy been fully taken into account?
- Will a robust privacy notice/signage be in place outlining the existence of surveillance and the use of personal data?
- Is personal data collected only to be used for the purposes outlined?
- Is only the minimum data required to fulfil the purpose collected?
- If applicable, is recording of audio data suitably justified? Has a ‘pressing need’ for audio been clearly articulated? Is there no other alternative?
- Has a Data Protection Impact Assessment (DPIA) been completed, and this checklist appended?

Security

- Is security of images assured from capture to destruction?
- Is access to view data confined to a secure area/office?
- Has the solution to be used been risk assessed (by IT&D)?
- Are all operator staff security cleared?
- Have operational, technical and competence standards been considered and adhered to e.g., applicable BSI standards?

Procedure and Governance

- Are robust procedures in place to ensure authorised access only?

- Is a contract in place with any third party supplier that assures compliance with data protection law?
- Do procedures clearly outline who, how and when personal data should be accessed, stored, and disclosed?
- Are all operator staff trained in relevant procedures including access, disclosure (inc. subject access) and retention?
- Are staff aware of the consequences of the misuse of surveillance technology?
- Will the use of surveillance be reviewed annually?
- Is there an Information Asset Owner identified?
- Is information kept only for as long as required to fulfil the purpose for processing?
- Is the operator of the surveillance technology suitably licenced?
- Can surveillance be ‘turned off’ when not required?
- Can data subject rights be met e.g., erasure?

Technical

- Is the accuracy and integrity of information assured? Does image quality and metadata (e.g., date and time) meet requirements for processing the data?
- Can images be pixelated for disclosure/subject access purposes?
- Do systems allow ease of disclosure where relevant?
- Is an audit of access and disclosure to be kept?
- Can data be made available in a commonly used format?
- Does positioning of cameras/surveillance equipment exclude areas where individuals would have a legitimate expectation of privacy?
- Do disclosure mechanisms allow secure delivery to intended recipients?
- Where both audio and visual recording is in place, can these be enabled independently e.g., can audio be switched on and off?