Surveillance Camera Policy

1 Version History details and author

1.0	24/02/2020	Draft prepared and reviewed by GDPR Task Group.	GDPR task group
2.0	11/05/2021	Reviewed and agreed by Information Governance Group.	Jane Lakin
3.0	07/03/2023	Approved and agreed by Information Governance Group, updated to reflect Surveillance Camera Code of Practice.	Jane Lakin/ Aaron Needham
4.0	10/10/2023	Approved by Information Governance Group. Drones and CCTV in taxis added.	Sinead Roberts

This document has been prepared using the following ISO27001:2022 standard controls as reference:

A.5.15 > 18 - Access Control
A.5.31 > 36 – Compliance
A.7.1 > 14 - Physical and Environmental Security

2 Introduction and Purpose

2.1 Derbyshire County Council ('the Council') operates and manages a number of Surveillance Cameras, Closed Circuit Television (CCTV), Body Worn Camera (BWC) and drones systems across its property estate. The camera systems are operated for the purposes of:

- Protecting the health and safety of employees and visitors to sites;
- Protecting service users.
- Acting as a deterrent to criminal or other poor behaviour and providing vital evidence in situations where an incident has been reported.
- Preventing and detecting crime or criminal activity, and protecting Council buildings and assets from damage, disruption, vandalism or other criminal activity;
- Creating a safer environment and providing reassurance to employees and the general public;
- To protect council buildings, workers, land and other public buildings
- Improving traffic management;
- Countering terrorism;
- Assisting with investigations, where appropriate;
- Assisting in the effective resolution of any disputes or legal or insurance-related claim involving the Council or Council personnel.

2.2 The Council is mindful of the need to balance public protection against individuals' right to respect for private and family life set out in Article 8 European Convention on Human Rights (ECHR), and consequently CCTV is only used where it is justified, necessary and proportionate, and only where there are no less privacy-intrusive methods available.

2.3 Camera systems are owned and managed by the Council or its approved suppliers. Under current data protection legislation the Council is deemed the 'data controller' for the images captured by its systems. If camera systems are jointly operated with partner agencies or with other suppliers the governance and accountability arrangements should be 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.

2.4 The Council's Head of Facilities Management is responsible for the overall management and operation of the camera systems, including activities relating to installations, recording, reviewing, monitoring and ensuring compliance with this Policy.

3 Relevant Legislation

3.1 The Council has a duty to comply with relevant legislation with regards to the installation and operation of Surveillance Cameras,CCTV and BWC systems , which includes:

- The UK General Data Protection Regulation and Data Protection Act 2018;
- The European Convention on Human Rights (ECHR) and the Human Rights Act 1998;
- The Freedom of Information Act 2000;
- The Environmental Information Regulations 2004;
- Protection of Freedoms Act 2012;
- The Surveillance Camera Code of Practice (Updated 3 March 2022);
- The ICO's data protection code of practice for surveillance cameras and personal information;
- The Covert Surveillance and Property Interference Code of Practice (August 2018);
- Regulation of Investigatory Powers Act 2000 – *(Note: overt CCTV is not covered by this Act but is included as a means of defining the boundaries of overt/covert recording).*

3.2 Cameras will not be used to monitor staff or individuals in the ordinary course of lawful business in the area under surveillance. Managers are not permitted to use the cameras to observe staff working practices or time keeping to assist them in the day-to-day management of their staff.

3.3 Individuals will only be monitored covertly if there is reasonable cause to suspect a criminal offence or serious breach of discipline is about to be committed. This will only be permitted when authorised and may require the use of a Regulation of Investigatory Powers Act 2000 (RIPA) authorisation. Before any action of this nature is undertaken officers must consult the Assistant Director of Finance (Audit) and the Director of Legal and Democratic Services. Details of the Council's RIPA Policy can be found on the Council's website. Regulation of Investigatory Powers Act

3.4 Details on how personal information captured by the surveillance cameras is used, stored and shared, can be found on the Council's website under the CCTV Privacy Notice.

3.5 BWC are used by Derbyshire County Council. Officers use BWC to prevent and detect crime and for health and safety reasons.

4 Responsibility

4.1 The Head of Facilities Management is the Council's Single Point of Contact (SPOC) in respect general enquiries, complaints and access requests for footage from the surveillance cameras. The Head of Facilities Management has responsibility for the deployment and management of surveillance cameras located on the Council's premises including the County Hall Complex in Matlock. The Head of Facilities Management will ensure that staff monitoring the cameras are properly trained in the use of the equipment and comply with the relevant Codes of Practice and Council procedures.

4.2 The Head of Facilities Management will provide guidance and support to departments in respect of surveillance camera use at the Council's satellite sites.

4.3 The Head of Facilities Management will be responsible for ensuring all users are kept up to date with current legislation and changes in operational procedures. The Surveillance Camera Policy will be subject to annual review and approval by the Council's Information Governance Group.

5 Procurement and Deployment of CCTV Cameras

5.1 The Council is committed to supporting an individual's right to privacy and this should always be a primary consideration in the operation of any surveillance system. Consideration must be given to the necessity for cameras within a location and their impact on the privacy of individuals using these areas. The Council will have regard to the Surveillance Camera Commissioner's guidance on relevant British, European and International standards when considering the procurement of surveillance cameras.

5.2 Under normal circumstances, cameras must not to be installed in such a way that they can look onto private property i.e. houses. Steps will be taken to ensure that the cameras do not view areas that are not intended to be the subject of surveillance. Where surveillance is intended to be overt, all cameras must be visible and signed appropriately.

5.3 Covert or unsigned cameras within the Council's property may on rare occasions be deployed in areas of high security where there is no legitimate public access and where staff access is controlled and restricted. Staff who normally work in these areas must, where appropriate, be informed of the location of these cameras and their purpose.

5.4 No member of staff, Department or Service is permitted to purchase and install a surveillance camera until a full Data Protection Impact Assessment (DPIA) has been completed. Before deciding on surveillance cameras, departments must take into account the nature of the problem they are seeking to address, whether a surveillance system would be a justified and an effective solution, whether better or less intrusive solutions exist, what effect its use may have on individuals, and whether in the light of this, its use is proportionate. Surveillance systems should also be regularly reviewed to evaluate whether they are still necessary. Details of the Council's DPIA Procedures can be found on the Council's website.

5.5 It is a requirement under the Surveillance Camera Commissioner's Code of Practice that any equipment purchased is fit for purpose and will meet the objectives of the completed DPIA. It is important that an effective maintenance schedule is in place to ensure the cameras are fully operational and satisfy the objectives for which they were initially installed. i.e. suitable picture quality.

5.6 Derbyshire County Council does not deploy 'dummy' cameras as these give a false sense of security.

6 Drones and Body Cameras

6.1 The Council may use drones to gather information for flood maps and flood risk situations, emergency response, severe weather, roads and infrastructure development. In such cases their use will be subject to completion of a Data Protection Impact Assessment (DPIA).

6.2 The use of body worn cameras will only be considered in the following circumstances and following the completion of a Data Protection Impact Assessment (DPIA):

- If an employee may be in a confrontational situation where they are subject to, or feel that they are likely to be subject to, verbal or physical abuse;
- To gather evidential footage for a Police or Council enforcement investigation.

Body worn cameras will not be used when performing normal or routine work and any usage must be proportionate, legitimate, necessary and justifiable in regard to the relevant law and policy.

7 Fleet Vehicle Cameras (Dash Cams)

7.1 Derbyshire County Council has some vehicles with CCTV fitted within the vehicle for reasons outlined in this policy. Where this is the case, there will be clear signage so that any occupants of the vehicles will be aware of any CCTV coverage and no sound will be recorded.

8 Security of Surveillance Cameras

8.1 Surveillance Camera Systems must be compliant with the Council's Password Policy. Default user accounts must be disabled and accounts for staff that have left the Council promptly removed. System Administrator Passwords for CCTV systems should be held in a secure system such as Password Manager Pro. Uncontrolled remote access to the surveillance camera system must not be permitted under any circumstances.

8.2 Surveillance Camera Systems must be compliant with the Council's Encryption & Cryptographic Controls Policy Encryption & Cryptographic Controls Policy to protect the storage of the camera images used at the Council's premises Where images are transmitted over the Internet (encryption in transit) (e.g. to allow viewing from a remote location) these connections must be encrypted as a security measure against interception and require some form of authentication for access (e.g. a username and secure password). Systems which make use of wireless communication links (e.g. transmitting images between cameras and a receiver) must ensure that these signals are encrypted to prevent interception.

8.3 Surveillance camera systems must have a process in place that enables security updates to be applied to ensure critical security vulnerabilities are addressed. Wherever possible, the process should be automated and undertaken in accordance with the Council's Network Security Policy.

8.4 Third party suppliers used to install and monitor surveillance cameras must be required to comply with the Council's Supplier Information Security Policy and have a written contract in place. The contract must clearly define each party's responsibilities and include guarantees about security, such as storage and the use of properly trained staff.

8.5 Where third party operatives are contracted to monitor public spaces, they will be required to hold a valid licence from the Security Industry Authority (SIA Licence).

8.6 Access to the surveillance camera recording equipment and footage must be restricted to authorised employees only and not available to the general public. Monitoring rooms must not enable unauthorised viewing from outside of the office with appropriate security controls put in place to protect staff and surveillance camera equipment.

8.7 Visitors requiring access to the Council's surveillance cameras or the recording equipment must sign in prior to being provided access.

8.8 When left unattended, the surveillance camera recording equipment must be secured at all times i.e. office or cabinets holding the devices kept locked.

9 Retention of images

9.1 Unless required for evidential purposes or other legal reason (such as to comply with an individual rights request) the investigation of an offence or as required by law, images will be retained for no longer than 30 days from the date of recording, in compliance with the corporate property retention schedule. Images after this point must be automatically overwritten.

9.2 Until the camera footage is overwritten, it must be stored securely on the Council's servers, cloud storage facility or the digital video recorder (DVR) hard drives with permissions set to authorised staff only. Physical copies of footage from the cameras such as printed images or footage copied to disc, are also subject to this Policy and the retention schedule and must be secured at all times.

10 Use of camera images

10.1 In circumstances where camera footage has been accessed, retrieved, recorded, viewed or disclosed a record must be maintained. Routine access should be recorded in an audit log, retained for six months in accordance with the Operational Management Policy. The log should give the identity of each user and the date and time on which footage was accessed. Exceptional

access for purposes of downloading, manually deleting, exporting or disclosing footage should be documented in the record of the associated activity. For instance, access to footage for a Subject Access Request (SAR) should be documented as part of the SAR record. The record must detail why the footage was accessed, the timeframe of the images, camera location, by whom and for what purpose.

11 Signage

11.1 All areas where surveillance cameras are in use must be clearly signed to comply with the data protection legislation unless the surveillance is covert. This is to inform individuals that they are about to enter an area covered by cameras or to remind them that they are in an area covered by surveillance. The signage will confirm that the systems are managed by the Council and include a 24 hour contact number for the Council. The signs will also act as an additional deterrent. Signs must not be displayed in areas which do not have surveillance cameras.

11.2 Where 'Covert' cameras have been authorised for deployment, signage will not normally be erected.

11.3 The signs must carry an image of a surveillance camera and Council's or partner Logo. The information on the sign must explain why the cameras are there, who manages them and a contact number, along with the URL of the CCTV privacy notice. The signs, position and the message needs to be large enough to enable individuals to easily read the information on it.

12 Employees Managing Surveillance Cameras

12.1 Operation and monitoring of the Council's surveillance cameras is restricted to authorised employees or contractors only. The Council ensures these employees and contractors are aware of the competency standards required by the Surveillance Camera Commissioner and are trained in respect of legislation appropriate to their role.

12.2 The Council must regularly monitor and maintain its surveillance camera systems to ensure continual compliance with the data protection legislation and that the images are of sufficient quality.

12.3 The cameras and recording systems are subject to an annual review to ensure they remain fit for purpose.

12.4 All maintenance issues must be reported to the Head of Facilities Management for investigation.

13 Surveillance Camera Information Sharing

13.1 All reasonable steps must be taken to prevent the loss, misuse or alteration of surveillance camera images. Information is only shared with third party organisations in accordance with the Information Sharing Policy and

Guidance, which will typically require an information sharing agreement to be in place.

13.2 Where footage is to be disclosed to a third party, consideration should be given to whether the identifying features of any of the other individuals in the images should be obscured.

13.3 Where it is envisaged that footage may need to be shared with a third party such as the Police, it is important to ensure that it is in a format that can be easily shared with and used by the third party.

13.4 Disclosure of information from surveillance camera systems must be controlled and consistent with the purpose(s) for which the system was established unless there is another lawful reason, such as for law enforcement purposes.

14 Central Register of Surveillance Cameras

14.1 In order to assist the Council to meet its legal obligations in respect of surveillance camera use, a central register will be maintained. The register will be held by the Head of Facilities Management and shall include:

- The physical location of each camera;
- The location of camera images i.e. cloud storage, internal server or DVR hard drive;
- The purpose and reason for use of each camera (DPIA);
- The responsible department and officer for the camera;
- Type of images being captured including night vision and voice capture;
- A statement from the DPIA of the necessity for the camera at that location;
- The details of any third party with responsibility for operating, monitoring or maintaining the system.

15 Applications for Disclosure of Images

15.1 Requests by individual data subjects, or a third party on behalf of an individual, for images relating to themselves should be responded to in accordance with the Council's Access to Information Procedures. Where there is any concern over whether the information should be disclosed, for instance if it forms part of an investigation into the individual making the request, advice should be taken from Derbyshire County Council's Data Protection Liaison Officers.

15.2 In order to locate the images on the Council's camera systems, 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.

15.3 Where the Council is unable to comply with a SAR without disclosing the personal data of another individual who is identified or identifiable from that information, it may not be 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.

16 Access to and Disclosure of Images to Third Parties

16.1 A request for images made by a third party should be referred to the Head of Facilities Management. 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. Such disclosures will be made at the discretion of the Head of Facilities Management, with reference to the Information Sharing Policy and Guidance, relevant legislation and where necessary, following advice from the Council's Legal Services Section.

16.2 Where a suspicion of misconduct arises and at the formal request of an Investigating Officer, Internal Audit or HR Manager/Advisor, the Head of Facilities Management may provide access to camera images for use in staff disciplinary cases.

16.3 A record of any disclosure made under this Policy will be held on the surveillance camera management system, itemising the date, time, camera, requestor, authoriser and reason for the disclosure.

17 Requests for Images by the Council's Employees

17.1 For activities which are work related, the matter must be referred to the appropriate line manager in the first instance to check if there are adequate grounds for the request which correspond with the Council's objectives for the use of surveillance cameras. If the manager deems the grounds to be appropriate, then the request should be referred to Head of Facilities Management to investigate further. Any requests which result in the access, viewing or release of footage must be recorded.

18 Inspections/ Visits

18.1 All surveillance cameras may be subject to inspections or visits by a member of the Information Commissioner's Office, Investigatory Powers Commissioner Office (IPCO) or the Council's staff including Internal Audit.

18.2 These visits/ inspections are designed to ensure that the systems are operating in accordance with current legislation, this Policy and or other Codes of Practice.

19 Copyright

19.1 Ownership of all footage recorded from the surveillance cameras will remain with the Council, including copyright where applicable. However, once there has been disclosure of footage to another body such as the Police then the

recipient becomes responsible for their copy of that footage and must comply with all applicable legal obligations.

20 Complaints

20.1 Any complaint made about the Council's use of the surveillance cameras or any other matter connected to the deployment of the cameras should be directed to the Head of Facilities Management in the first instance and dealt with in line with the Council's Corporate Complaints Procedure.

20.2 All complaints about subject access requests should be notified to the Access to Information Officer (AIO) who will determine the appropriate next steps. The AIO maintains a record of all requests for internal reviews and complaints which are escalated to the Information Commissioner's Office. This data is shared with the Council's Data Protection Officer and reported to the Council's Information Governance and Implementation Groups to facilitate trend analysis and improve working practice.

21 Breaches of Policy

21.1 Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Council information assets, or an event which is in breach of the Council's security procedures and policies. All third party suppliers contracted to provide, support or access solutions, which enable the Council to carry out its business functions and deliver its services, have a responsibility to adhere to this policy and all supporting requirements as described and referenced within formal documentation and agreed contractual agreements.

21.2 All employees, elected members and volunteers have a responsibility to report security incidents and breaches of this policy immediately on becoming aware of the incident through the Council's Incident Reporting Procedure Report a security incident - Our Derbyshire.

21.3 In the case of third party vendors, consultants or contractors, non-compliance could result in the immediate removal of access to IT solutions or suspension/ termination of contractual arrangements. If damage or compromise of the Council's IT solutions or loss of information results from the non-compliance, the Council will consider legal action against the third party. The Council will take appropriate measures to remedy any breach of this policy and its associated procedures and guidelines through the relevant contractual arrangements in place or otherwise via statutory processes. In the case of an employee, infringements will be investigated under the Council's disciplinary procedure and progressed as appropriate.

Appendix 1

Surveillance Camera Commissioner - Code of Practice - Steps to complying with the 12 principles