Swindon Borough Council
CCTV & Surveillance Camera Policy

1. Policy Statement

Surveillance Camera systems are used as a valuable tool to assist with public safety and security, enforcement of legislation and to protect property. Swindon Borough Council (SBC) will operate its systems to the requirements of Data Protection legislation and good practice guidelines, such as those issued by the Information Commissioner's Office (ICO) and the Surveillance Camera Commissioner (SCC), to ensure the need for public protection is balanced with respect for the privacy of individuals.

2. Scope

This policy applies to all overt (open) CCTV installations controlled by or on behalf of the council, including both internal and external cameras, dashcams, Automatic Number Plate Recognition (ANPR) and Body Worn Cameras (BWC) utilised by enforcement officers and employees with similar, relevant, roles. These are referred to throughout this policy collectively as surveillance cameras.

This policy also covers the use of Unmanned Aerial Systems (UAS) equipment should the council decide, at any point, to utilise this technology.

This policy does not apply to the covert (secret) use of surveillance cameras, which is covered by the Regulation of Investigatory Powers Act 2000 (RIPA). .

3. Legislative and Governance Framework

- Data Protection Act 2018
- UK GDPR
- Human Rights Act 1998
- Freedom of Information Act 2000 Protection of Freedoms Act 2012
- Private Security Industry Act 2001
- 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).
- Information Commissioner's Office - Code of Practice on CCTV
- The College of Policing Guidance on body worn cameras 2014
- Surveillance Commissioner Code of Practice

4. Purposes

4.1 Primary Purposes

The Council's Security Manager and Data Protection Officer must be consulted before any surveillance camera system is implemented or altered.

Surveillance camera systems will only be implemented where they will assist the Council to meet one or more of the following purposes:

1. Deter and detect criminal activity;
2. Maintain public order;
3. Increase security by monitoring of activity within the council's properties, both to the exterior and interior of the buildings and access to car parks;
4. Address levels of anti-social behaviour;
5. Keep people safe;
6. Help to protect officers at work (for Health and Safety purposes);
7. Help prevent acts of aggression or verbal and physical abuse or assault to council or contractor staff;
8. Enforce legislation, including parking and driving restrictions;
9. Improve services to the public;
10. Understanding traffic flows and road safety issues;
11. Provide evidence to support insurance or internal investigations (complaints) andin cases of alleged illegal activity.

4.2 Secondary Purposes

Once it has been established that there is a need for a surveillance camera system for one of the above purposes, the information (including images) collected may also be used for the following purposes:

1. Help investigate breaches in Health and Safety incidents, complaints, legal matters and grievances;
2. Assist in the investigation of allegations of inappropriate conduct by officers;
3. As evidence in criminal proceedings (in this case the information may be provided to the police);
4. For insurance purposes, including the investigation of claims;
5. For audit and quality assessment purposes;
6. To improve the quality of services, for example to identify training needs.

Any request that does not fall within the above will be considered and a decision taken if it is a proportionate use of CCTV by the Security Manager and the Information Governance Manager.

Any intended use for any covert purpose must only take place after the accountable officer is satisfied that a completed Regulation of Investigatory Powers Act 2000 (RIPA) authorisation signed by a senior police officer or a magistrate is in place. The accountable officer must keep a copy of the authorisation for their records.

5. Operation

Surveillance systems will be operated fairly within all applicable laws, and only for the purposes stated in this policy.

The council will not locate surveillance cameras in positions that would record sensitive things like intimate care or people privately observing religious beliefs.
There will be a named accountable officer for each surveillance camera system.

The accountable officer for each system will ensure there are operating procedures in place, which are clearly documented, monitored and understood by operators.

6. Data Protection Impact Assessment

The Council respects and supports an individual's entitlement to go about their lawful business and this will be a consideration in the operation of a surveillance system. Although, it is recognised that there is inevitably some loss of privacy when surveillance systems are operational.

A data protection impact assessment will be completed for each surveillance system, to help identify whether something else could be done that would intrude less on people's privacy and whether surveillance is the best way to use resources.

7. Privacy Notices

To ensure that individuals are made aware of the surveillance cameras privacy notices the council will implement:

- Signs advising of the use of surveillance cameras, when located in a fixed or regularly used location
- Privacy Notices on the council's website

In instances where Body Worn Cameras (BWC) are to be used, and where practical, operators will inform the individual (or group) that the BWC is switched on and recording. There may be occasions when to do so would escalate the incident or put the operator in danger if such a warning was given, but this should be very rare and the operator may be required to justify such an action.

Individuals will only be continuously monitored if there is reasonable cause to suspect an offence or serious breach of discipline has been, or may be, about to be committed.

BWCs will not be used to monitor the progress of individuals in the ordinary course of lawful business in the area under surveillance.

8. Retention of data

Each surveillance camera system will identify a retention period for the images/sounds that are captured. These will be recorded in the Council's Retention & Disposal Policy.

Where information is requested for legal, civil or criminal investigations and proceedings the council may seek to extend the retention period for any relevant information.

9. Access Rights

If a member of the public has been identified as being recorded by the council they can request to view the recording. The request will be treated as a subject access request under The Data Protection Act 2018. More details about Subject Access Requests and information rights can be found on the Council's website.

Availability of the recordings will be subject to the retention period for that system. Recorded material will not be sold or otherwise used for commercial purposes or the provision of entertainment.

No images captured by surveillance cameras are to be released to other organisations until the Council has received and validated a signed request under Data Protection Act, outlining and justifying the request for the images.

Public showing of recorded material will only be allowed in compliance with enforcement agencies' needs connected with an investigation and only then in accordance with the Codes of Practice of The Police and Criminal Evidence Act 1984, or any other circumstance provided by law.

The Subject Access requests pages on the Swindon Borough Council website can be found at Subject Access Request Page

If the Subject Access Request is agreed copies of the relevant CCTV is provided once editing has taken place to remove or obscure the identify other non-relevant individuals in the CCTV requested.

Where Police request CCTV images, these are dealt with under sharing protocols in place via the GDPR Data Sharing Code.

10. Data Quality (quality of images)

The quality of recordings must be sufficient to satisfy evidential requirements and data protection requirements.

It is important that the images produced by the equipment are as clear as possible in order that they are effective for the purpose(s) for which they are intended.

Data recorded by surveillance cameras must be easily retrieved, such as through the use of date, time and location stamps.

Recorded material should be stored in a way that maintains the integrity of the image. This is to ensure that the rights of individuals recorded by the surveillance camera system are protected and that the material can be used as evidence if required.

Still photographs of surveillance camera images must not be taken as a matter of routine. The taking of each photograph must be capable of justification (for example for the prevention or detection of crime and anti-social behaviour) and only done so with the permission of the named accountable officer in charge of the surveillance camera system.

11. Audio recording

Surveillance cameras with audio should not be installed unless found to be proportionate following a Data Protection Impact Assessment. Where it is deemed necessary to capture audio, signage and procedures will reflect this.

Any surveillance camera installed with the ability to make audio recordings not found to be proportionate will have this facility switched off.

12. Data Security

Organisational and technical measures must be put in place to ensure the security of the equipment, monitors and recordings, including:

- Appropriate training for surveillance camera operators;
- Restricted access to surveillance camera footage on a need to know basis;
- Secure location of monitoring equipment and footage, surveillance camera monitors need to be in a lockable office and available to authorised persons only;

- Ensure the location of surveillance cameras does not capture financial card transactions and complies with the Card Payment Policy;
- Strong passwords to protect information, using the Council's Password Policy; Hosting that complies with Data Protection and the council's information security requirements;
- Documented procedures for when people ask for access to recordings, about sharing information and for complaints about surveillance;
- Audit trail records of who has had access to the information, when and why;
- Documented procedures for keeping information and recordings secure, how long they are kept for, and when and how they are destroyed;
- If someone else (like a security company) is handling personal data on the Council's behalf, the contract with them must set out clear rules on how they process it; and
- The recording system should be checked and maintained on a regular basis to ensure it is in good working order.
- Where the processing of surveillance camera data is carried out by a third party, this must be done in accordance with this policy and the Council's Data Protection and Security policies.

13. Licensed Operators

Any third party company employed to guard our premises or act as a keyholder must hold the relevant Security Industry Authority (SIA) licence.

Where an employee is undertaking surveillance of a public or private space for the purposes of providing a service, then the relevant licence will be required. For example – if a third party occupying part of our premises and the council has contractually agreed to provide a security service (including surveillance cameras), the council will apply for a licence.

Should the council alter its office accommodation strategy to include a 'serviced' element to third parties in the future, the SIA licensing requirements would need to be met.

14.Images obtained from other sources

Services may obtain images captured by surveillance systems operated by other agencies (Police and Parish Council CCTV for instance). The security and management of these images will need to be considered. The retention period for the purpose it was needed by the council will apply, for example if it relates to a child protection investigation the images will need to be kept for the same length of time as the remainder of the investigation records.

15. Specific Responsibilities

15.1 Commissioners and Contract Managers

If you are a commissioner of an external service provider or are managing the relationship with a partner who is managing a surveillance camera system on behalf of the Council, you must ensure the third party complies with this policy and supporting procedures, Data Protection legislation and the Surveillance Commissioner's Code of Practice.

Your considerations need to include:

- How easy is it to take copies of a recording off the system when asked for by a law enforcement agency or in response to an individual rights request?
- Can this be done without interrupting the operation of the system?
- Are recorded images straightforward to use/share? Does the system allow you to blur out other individuals in the recording?
- How you will manage a situation where recorded material needs to be taken away for further examination and any potential impact this may have on the operation of the system?
- If the system records features such as the location of the camera and/or date and time reference, how this will be maintained to ensure accuracy.
- Building regular maintenance of the cameras into the contract in order to ensure the clarity of the images recorded.
- In certain circumstances, the service provider might need to hold a licence issued by the Security Industry Authority. Where appropriate, this should be clarified with the service provider at the outset.

15.2 Information Asset Owners (IAOs)

IAOs are accountable for ensuring their surveillance systems meet the requirements of the law and council policy and standards and are captured in the council's Information Asset Register.

15.3 Security Manager

The Council's Security Manager, together with the Data Protection Officer as SRO for the Protection of Freedoms Act 2012 will determine the equipment, procedures and processes for managing and operating surveillance systems for council buildings, across the estate.

The Security Manager is responsible for ensuring that operatives of surveillance systems on council buildings are aware of and understand their responsibilities.

The Security Manager is responsible for managing any contract(s) for surveillance systems on council buildings.

15.4 Operators

If your role at the council includes the monitoring or operation of surveillance cameras, you must;

- Have an appropriate level of operational knowledge and training for surveillance camera operators; ie SIA cctv licence
- Complete the council's annual mandatory Data Protection & Information Security e learning as a minimum training level; Are familiar with and implement:
    - System specific security and information management procedures and retention periods;
    - Corporate processes for individuals' rights and access requests, and access requests from third parties and enforcement agencies.
- Follow corporate and/or departmental policy, procedures and guidance on the operation of surveillance camera systems; and
- Implement appropriate physical security, where required, to assure the integrity of the surveillance camera systems and their recordings.

16. References

The Council's website includes a CCTV page: https://www.swindon.gov.uk/info/20029/people_and_communities/1048/cctv_in_swindon

17. Policy Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 3 years.

18. Document Control

Author:	
Owner:	J
Approval body	***Information Governance Board***
Date approved	
Document Number:	V1.0

19. Version History

Version	Version Date	Summary of Changes
V1.0	*September 2021*	*New policy*