information management & security

Gloucestershire COUNTY COUNCIL

CCTV and Surveillance Policy

1.0 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. Gloucestershire County Council (GCC) 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.

2.0 Scope

This policy applies to all overt (open) CCTV installations controlled by or on behalf of the council, including internal and external cameras, dashcams, Automatic Number Plate Recognition (ANPR) and Body Worn Cameras 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 drones should the council decide to utilise this technology in the future.

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

3.0 Legislative and Governance Framework

- Data Protection Act 2018,
- 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 (which does not cover open CCTV, but is included in this policy as a means of defining the boundaries between overt and covert recording),
- Information Commissioner's Office Code of Practice for CCTV,
- The Surveillance Camera Commissioner's Code of Practice for CCTV,
- The College of Policing Guidance for Body Worn Cameras 2014.

4.0 Purposes

4.1 Primary Purposes

The Information Management Service (IMS) must be consulted before a surveillance camera system is installed, altered, or expanded.

Surveillance camera systems must 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 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 councillors and staff at work (for Health and Safety purposes),
7. Help prevent acts of aggression or verbal and physical abuse including, assault to councillors, staff, and contractors,
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 (such as complaints) and in cases of alleged illegal activity.

4.2 Secondary Purposes

Once it has been established that there is a need for a surveillance camera system, the information collected (including images) 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 staff or councillors,
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 (such as identifying training needs and supporting training exercises).

Any intended use of surveillance cameras for the purpose of covert surveillance can only take place once authorised in line with the council's Covert Surveillance Procedural Guidance and with judicial approval where appropriate, in line with the Regulation of Investigatory Powers Act (RIPA) 2000.

The authorising officer must keep a copy in the central record of authorisations.

5.0 Operation

Surveillance camera systems must be operated fairly within all applicable laws, only for the purposes stated in this policy and with due regard to the principle that everyone has the right to respect of their private life.

The council will not locate surveillance cameras in positions that would record sensitive activities such as intimate care or people privately observing religious beliefs.

The public interest in the operation of our systems will be recognised by ensuring the security and integrity of operational procedures.

There will be a named accountable officer for each surveillance camera system who will ensure operating procedures are in place and are clearly documented, monitored, and understood by operators.

6.0 Data Protection Impact Assessment

The council respects and supports an individual's entitlement to go about their lawful business, which 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 use of resources.

7.0 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 a group of individuals) 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 this warning is 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.

8.0 Retention of Data

Each surveillance camera system will identify a retention period for recorded footage and audio (where audio functionality is deemed proportionate). These will be documented in the council's retention schedule.

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

9.0 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 an individual's information rights can be found on our website.

No images captured by surveillance cameras are to be released to other organisations until the council has received and validated a signed request under the Data Protection Act 2018, outlining and justifying the request for the images.

Public showing of recorded material will only be allowed in compliance with an enforcement agency's needs in connection with their 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.

All requests for information from members of the public and enforcement agencies, and statutory requests from other agencies, must be shared with IMS before they are responded to.

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.

10.0 Data Quality (Quality of Images)

The quality of recordings must be sufficient to satisfy evidential and data protection requirements. It is important that the images produced by the equipment are as clear as possible to ensure they are effective for the purpose(s) for which they are intended.

Recorded material must be easily retrieved (for example, date, time, and location stamps) and 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. Capturing still photographs must be justified (such as the prevention or detection of crime and anti-social behaviour), and only taken with the express permission of the named accountable officer in charge of the surveillance camera system.

11.0 Audio Recording

Surveillance cameras with audio should not be installed unless found to be proportionate following the completion of a Data Protection Impact Assessment (DPIA). 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.

12.0 Data Security

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

- Appropriate training for surveillance camera operators,
- Restricted access to surveillance camera footage on a need-to-know basis,
- A secure location for monitoring equipment and footage (surveillance camera monitors need to be in a lockable office),
- Ensuring the location of surveillance cameras does not capture financial card transactions and complies with the Card Payment Policy,
- Strong passwords to protect information in line with 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,
- 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 (such as a security company) is handling personal data on the council's behalf, the contract must set out clear rules on how the information is processed; 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 the Cyber and Information Management (Procurement) Policy.

13.0 Licensed Operators

Any third-party company employed to guard council 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 occupies council 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.

14.0 Images obtained from other sources

Where appropriate, service areas may request/obtain images captured by surveillance systems operated by other agencies (such as the police and district councils). The security and management of these images must be considered at all times.

Any images obtained from other sources to support a council-led investigation should be retained in line with the remainder of the investigation records.

15.0 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 agency 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 from the system when asked 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 or share? Does the system allow you to blur out other individuals in the recording?
- How will you 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 the location of the camera, the date and time, how will this be maintained to ensure accuracy?
- Building regular maintenance of the cameras into the contract 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, the council's policies and standards, and are recorded in the council's Information Asset Register.

15.3 Asset Management and Property Services (AMPS)

AMPS will determine the equipment, procedures, and processes for managing and operating surveillance systems for council buildings across the estate.

AMPS are responsible for ensuring that surveillance camera operators on council buildings are aware of, and understand, their responsibilities.

AMPS are responsible for managing the contract for surveillance systems on council buildings.

15.4 Operators

If your role includes operating, maintaining, or implementing surveillance cameras systems as a direct responsibility, or in addition to your normal duties, it is essential that you:

- Ensure compliance with data protection legislation and the council's Data Protection Policy, where relevant, for the operation of surveillance camera systems,
- Have an appropriate level of operational knowledge and training for surveillance camera operators,
- Complete the council's 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.

16.0 Audits, Inspections and Reviews

The council's surveillance camera systems are subject to internal and external audits, inspections, and reviews, including:

- Ad-hoc spot checks,
- Annual reviews,
- An examination of monitoring room records and recorded footage,
- Data captures to calculate the number of systems in operation, as well as the make and model number for every camera used to support these systems,
- External surveys and audits from CCTV regulators, such as the Surveillance Camera Commissioner (SCC), and
- Reviews of the completed DPIAs and Self-Assessments for each system.

The council and its partners will co-operate fully with the requirements of all audits and inspections and will ensure that learning and adjustments are applied to improve practice and compliance.

17.0 References

This policy and other related information security policies and standards can be found at Information Management and Security Policies.

18.0 Document Control

18.1 Document information

Owner:	Jenny Grodzicka, Head of Information Management Services (DPO)
Author:	Jenny Grodzicka, Head of Information Management Services (DPO)
Reviewer:	Jenny Grodzicka, Head of Information Management Services (DPO)
Date created:	January 2021
Next review date:	October 2025
Approval:	Information Board, November 2022 (v2.0)
Version:	2.2
Classification:	UNCLASSIFIED

18.2 Version History

Version	Version date	Summary of Changes
1.0	January 2021	First version. New policy developed. Consultation undertaken with key stakeholders in the council, including RIPA and Legal Services representatives. Approved by Information Board, February 2021.
1.1	February 2022	Inclusion of use for protection of councillors.
2.0	November 2022	Additional information added in section 5, aligning policy to SCC's code of practice. Section 16 added reflecting the council's responsibilities in relation to audits, inspections, and reviews. Accessibility review, and updates to formatting. Broken links fixed, link to Data Protection Policy added in section 15.4. Approved by Information Board, November 2022.
2.1	November 2022	Section 4 has been amended to accurately reflect the use of cameras for covert purposes, in line with the Council's Covert Surveillance procedural guidance and the Regulation of Investigatory Powers Act (RIPA) 2000.
2.2	February 2024	Section 9 has been amended to reflect that access requests (from members of the public and enforcement agencies) must be shared with IMS before they are responded to. Secondary purposes (section 4.2) now covers training exercises. Broken links fixed. New link to Covert Surveillance Procedural Guidance added. Reviewer updated

18.3 Review

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

18.4 Contact Us

Post: The Information Management Service
Gloucestershire County Council
Shire Hall
Westgate Street
Gloucester
GL1 2TG
Email: dpo@gloucestershire.gov.uk
Phone: 01452 324000