Leicestershire County Council

Surveillance Camera Technologies Policy

Version: 1.0

Agreed by: DPO and SIRO

Date: December 2020

Review Date: December 2021

Document Control

Control Details

Document Location:	X:\Information and Technology\Policies and Procedures\01 Approved\Surveillance Camera Technologies\Products\Final
Production Software	Microsoft Word
Author:	Information Governance
Owner:	Information Governance

Document Amendment Record

Issue	Amendment Detail	Author	Date
0.1	Initial draft	RK	July 2019
1.0	Published version	RK	December 2019
1.0	Annual review – Minor changes	RK	December 2020

1 Introduction

Leicestershire County Council (the Council) operates and manages a number of surveillance camera technologies.

Subject to an annual assessment, the Council uses surveillance technologies for the purposes of:

- supporting the security of its premises;
- protecting the health and safety of the staff and those using its property;
- supporting the prevention and detection of crime;
- discouraging aggressive or violent behaviour towards staff and providing support if necessary;
- provide emergency services assistance; and
- managing traffic on Leicestershire's roads.

The Council maintains and operates most of the surveillance camera technologies it uses. However, it does operate some which are maintained by third parties. All systems operate within the requirements of the Data Protection legislation and good practice guidelines, such as those issued by the Information Commissioner's Office (ICO) and the Surveillance Camera Commissioner (SCC). The aim of the SCC code is to ensure that surveillance camera technologies are used in pursuit of a legitimate aim to meet a pressing need and that any impact on privacy is balanced against such aims. The ICO code provides good practice advice for those involved in operating CCTV and other surveillance camera technologies, including how organisations can meet their data protection obligations when using these devices.

The Council has adopted both the ICO Data Protection Code of Practice and the Surveillance Camera Code in full and the principles of the Surveillance Camera Code set out in Appendix 1, are incorporated into this policy.

2 Scope

This policy applies to all overt (open) surveillance camera (including audio technologies) controlled by the Council and utilised by enforcement officers and employees with relevant, roles. It covers live viewing of surveillance technology as well as replaying / reviewing footage / audio in response to a request.

If the Council introduces or considers introducing new forms of surveillance technology which capture personal data, for example unmanned aerial systems, the provisions of this policy will apply. The Council will consider whether this policy requires amendments to take into account new technology.

This policy does not apply to the covert (secret) use of surveillance camera technologies, which is covered by the Regulation of Investigatory Powers Act 2000 (RIPA). However, section 10 of this policy briefly covers RIPA in order to highlight the difference between covert and overt surveillance.

3 Policy Statement

The purpose of this policy is to:

- ensure compliance with relevant legislation, as listed in Section 6;
- ensure adherence to the Surveillance Camera Code of Practice (Section 30 of the Protection of Freedoms Act 2012);
- ensure adherence to the ICO CCTV Code of Practice;
- set out how surveillance technologies will be operated and monitored by the Council;
- outline the roles and responsibilities for the surveillance systems, their operation, monitoring, training, security and compliance.

4 Surveillance Camera Technologies

This policy shall apply to all forms of surveillance camera technologies (including audio technologies) operated by the Council including any that may be implemented in the future.
These technologies include the following:

- **CCTV -** static fully functional (including, pan, tilt and zoom) cameras, which may transmit images to a control, monitoring and/or recording facility, including cameras activated once triggered by motion;
- **Body Worn Cameras -** Cameras worn on the person, which may transmit images to a control, monitoring and/or recording facility;
- **Dash Cam's -** Vehicle mounted cameras which may transmit images to a control, monitoring and/or recording facility;
- **Automatic Number Plate Recognition (ANPR) -** Cameras, which capture and interpret the vehicle registration number of vehicles; and
- **Emerging technologies** which operate in a manner defined by this policy;
- **Surveillance technologies** that also include audio.

5 Relevant Legislation

With regards to the installation and operation of Camera Surveillance Systems, the Council must comply with all the relevant statutory legislation, in particular the following:

- Data Protection Act 2018
- General Data Protection Regulations 2016/679 (EU)
- Human Rights Act 1998
- Freedom of Information Act 2000, Protection of Freedoms Act 2012
- 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)
- Private Security Industry Act 2001 Of Practice 2013

- Information Commissioners Office (ICO) Data Protection Code of Practice for Surveillance Cameras and personal information.

6 Duties and Responsibilities

The Council is a Data Controller under data protection legislation and has responsibility for the fair and lawful processing of personal data, this responsibility rests with the Chief Executive on behalf of the Council as a whole.

Camera surveillance systems are within the scope of the data protection legislation because they capture personal data.

If your role includes camera surveillance systems, either as a direct responsibility or peripheral to your normal tasks, you are authorised to use surveillance systems as determined in this policy. It is essential that you understand and abide by the following appropriate responsibilities:

6.1 Manager Responsibilities

This section is aimed at managers that operate surveillance camera systems and / or are looking to procure new systems. Those managers have the following responsibilities:

- Where required, procuring new camera surveillance systems in conjunction with the Commissioning Unit, Property Services and Information Governance in line with corporate guidance (Buying and installing a new surveillance system guidance).
- Working with Information Governance to the create and approve a Data Protection Impact Assessment(s).
- Ensuring that Fair Processing Notices are up to date – work with IG where there are changes required.
- Ensuring that all policy, procedures and guidance on the operation of surveillance systems are implemented and followed.
- Liaise with ICT Services to ensure there is suitable ICT infrastructure in place.
- Annually review the requirement for the surveillance camera system in accordance with the SCC code of practice.
- Regular updating of 'local' system operating procedures.
- Ensuring that appropriate physical security is in place to assure the integrity of the camera surveillance systems and their recordings.
- Ensuring that access to data is strictly controlled and only made available to authorised personnel.
- Ensuring all staff who will use the system must read, understand and abide by the Surveillance Acceptable Use Policy.
- Identifying and implementing specific training for staff working with surveillance camera systems (operation, use and management of).
- Ensuring that the necessary controls are in place to safeguard compliance with the relevant legal requirements, guidance and policy.
- Follow appropriate processes when requests for footage are received – see section 9.
- Ensure correct signage is used on all surveillance system installations.

- Updating the Information Asset Register for new systems and maintaining the quality of information linked to camera systems in use.

6.2 Surveillance Operators' Responsibilities

Surveillance operators are defined as staff who, as part of their role, have a need to routinely use or access surveillance footage.

- Surveillance operators must read, understand and abide by the Surveillance Acceptable Use Policy.
- Complying with this policy and other Council data protection policies, departmental procedural guidance and any other relevant documentation when operating surveillance camera systems.
- Having an appropriate level of operational knowledge and training in the control, use and management of the surveillance camera devices.
- Undertake and complete any specific training linked to their duties and the camera technology being used.
- Ensuring that the surveillance camera devices are working on a day-to-day basis.
- Bringing defective equipment issues to the attention of the manager.
- Follow any local procedures and processes for the specific systems in use (e.g. signing out specific body cameras).
- Ensure that any member of staff asking you to use surveillance technology has identified a specific reason for the purpose for doing so. Suggested form in Appendix B to record this.
- Support appropriate processes when requests for footage are received – see section 9.

6.3 Information Governance Team Responsibilities

- Supporting the business in the development and approval of Data Protection Impact Assessments (DPIA's).
- Ensuring policy documentation related to camera surveillance and data protection legislation is up to date.
- Coordinating / investigating information incidents linked to camera surveillance systems.
- Supporting Subject Access Requests relating to surveillance images.
- Ensure wider ICT implications are considered.
- Ensuring compliance with operational procedures and that the purpose of the technology remains appropriate.

6.4 Commissioning Unit Team Responsibilities

- Supporting the business when procuring a surveillance system.

6.5 Property Services Team Responsibilities

- Ensuring we maintain a central register of all the Council's surveillance systems.

7 Storage and Security

Images and information will be stored in line with industry standards, relevant to the type of surveillance system installed.

Recorded images will be stored securely in digital format. Where there is a business reason to keep an image longer than the usual retention period, the image will be copied and stored securely in digital format, with a new retention period being documented. Where relevant, other Council policies may also govern how certain aspects of the Council's surveillance systems are used, for example the Information Security & Acceptable Use Policy.

Recorded images and associated information will only be used for the purposes defined for each installation. Surveillance images will only be viewed when there is a legitimate reason to do so and the showing of recorded material to other internal or external individuals will only be allowed in accordance with the law and the Surveillance Acceptable Use Policy.

8 Retention

Images that are not required for the purpose(s) for which the surveillance camera system is being used will not be retained for longer than is necessary and in any event no longer than 28 days. Access to and security of images will be controlled in accordance with the requirements of data protection legislation.

Security measures will be taken to prevent unauthorised access to, alteration, disclosure, destruction, accidental loss or destruction of recorded material.

9 Access Requests

Council departments, individuals staff members, or members of the public may request access to camera surveillance data. There are a number of different reasons for requesting access and for a range of different purposes. These differing requests will need to be considered in different ways.

Under data protection legislation, individuals have the right to access data the Council holds about them. All staff involved in operating a surveillance camera system must be able to recognise a request for access to recorded images by data subjects and be aware of an individual's rights. When a request (Subject Access Request) is made, the Council will handle it in accordance with data protection legislation and its Data Protection Policy.

Requests for images in connection with *current or prospective legal proceedings* may be permitted under Schedule 2 Paragraph 5 of the Data Protection Act 2018 (DPA) but careful consideration needs to be given to whether disclosure is necessary and proportionate.

Requests made by different statutory bodies for example the police, can be complied with using the exemption under Schedule 2, Part 1, Paragraph 2 of the DPA if it is satisfied that the reasons and statement of purpose, accord with the Scheme Purposes.

Camera surveillance images can be requested under the Freedom of Information Act 2000 (FOI). Personal information is usually exempt from disclosure under S40 of the Act but there may be instances where footage does not contain personal information and will need to be considered for release. Requests made under FOI must be handled in accordance with the Freedom of Information Process.

Guidance on making a request is available to members of the public and for members of staff.

More detailed guidance is also available for the teams that will process such requests. This guidance is designed to aid the review teams in setting out their own processes and procedures, in order to process surveillance data access requests while remaining within the requirements of data protection legislation.

The categories of requests covered include (but are not limited to):

- Freedom of Information Requests
- Subject Access Requests
- Internal (non-HR related) Requests
- HR related Requests
- Police, Courts, Legal or Insurance Requests
- Requests regarding Waste and recycling sites
- Traffic Cameras
- Parking Enforcement Cameras and Dashcams
- Town Centre Cameras
- Libraries and other Locality Buildings

Each of these categories of requests will need to be reviewed using differing processes and by different teams.

10 Regulation of Investigatory Powers (RIPA)

Targeted covert (secret) surveillance of individuals will only be undertaken for good reason, and in line with the procedures set out in the Regulation of Investigatory Powers Act (RIPA) Policy. Local authorities can only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment.

The viewing of everyday camera images is not considered to be covert recording and is therefore covered by this policy and not the RIPA process. This is because the camera is visible and appropriate signage is displayed in accordance with the Codes of Practice from the ICO & SCC. A decision to monitor a particular employee or

member of the public is considered to be targeted surveillance, which falls under RIPA (Regulation of Investigatory Powers Act 2000).

11 Policy Review

A review of this policy will take place annually or as required to take account of any new or changed legislation or regulations, business practices or new technology.

12 Breaches of this Policy

Inappropriate access use or disclosure of camera surveillance images may put members of the public, employees or camera surveillance operators at risk of serious harm, damage or distress. It may also put the Council at risk of reputational damage and / or be unlawful. Therefore, authorisation, access and disclosure of information will be strictly controlled, and any breaches of policy or operational guidance will be investigated.

Failure to adhere to this policy will place the Council at significant risk and may also result in a breach of legislation.

All breaches and suspected breaches of this policy **must be reported**, via your line manager, your department's I&T Business Partner, the ICT Service Desk or direct to Information Governance - informationgovenance@leics.gov.uk

Actions or neglect leading to a breach of this policy, or failure to report a breach will be investigated and may lead to disciplinary action.

13 Monitoring

All activity and information placed on or sent over Leicestershire County Council systems is monitored as defined by the Information Security and Acceptable Use Policy. Any logs created as part of this monitoring may be used to investigate suspected unauthorised use or breach of the Information Security and Acceptable Use Policy. For third party systems these logs must also be created and made available to the Council on request.

Appendix 1

The 12 Principles set out in the **Surveillance Code of Practice**:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be securely deleted once their purposes have been discharged.

7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

Appendix 2

Request to use CCTV for a specific purpose

The purpose of this form is to request an operator to perform a specific task with the surveillance footage being captured.

This form can also be used to request that a member of staff proactively looks at the stream of footage being captured if that is required for the safety of either the staff members or the service user. (Please note, this is not about the use of covert surveillance as there should already be clear signage used around the building).

Please note, it is the requestors responsibility that the purpose of the surveillance is lawful. If you are unsure about the lawful purpose, then please seek advice from the Information Governance Team.

Name of requestor	
Job title & Team name	
Department	

Reason for request	
Date of request	
Date and time of recording	
Duration of recording	

Purpose – tick all that apply.

Supporting the security of the premises	
Protecting the health and safety of the staff and those using the property	
Supporting the prevention and detection of crime	
Discouraging aggressive or violent behaviour towards staff and providing support if necessary	
Provide emergency services assistance	
Managing traffic on Leicestershire's roads	

If the purpose is not listed above, then please seek advice of your line manager and / or the Information Governance Team. If you need access to this footage, then you need to request this via the SAR process – please email SAR@leics.gov.uk.