# Leicestershire County Council

## CCTV Policy

Version v1.1

Agreed by: I&T Board

Date: April 2017

Review Date: April 2018

# Document Control

## Control Details

**Document Location:** X:\Information and Technology\Policies and Procedures\01 Approved\Caldicott Guardian\Products\Final

**Production Software:** Microsoft Word

**Author:** Policy and Assurance Team

**Owner:** Policy and Assurance Team

## Document Amendment Record

| Issue | Amendment Detail | Author | Date |
|---|---|---|---|
| 0.1 | First Draft | KM | 11 Nov 16 |
| 0.2 | First Draft | KM | 11 Nov 16 |
| | Second Draft | KM | 21 Jan 17 |
| 0.3 | Third Draft | KM | 13 Mar 17 |
| 1 | Final | KM | 24 Apr 17 |
| 1.1 | Transferred to new policy template | AP | 05 Jan 17 |

## 1. Introduction

Closed Circuit Television (CCTV) and Body Worn Video (BWV), is used by Leicestershire County Council. They are used as a valuable tool to assist with public safety and security and to protect property.

The CCTV installations and Body Worn Video are owned and maintained by Leicestershire County Council (the council) and are operated to the requirements of the Data Protection Act 1998 (DPA) and good practice guidelines, such as those issued by the Information Commissioner's Office (ICO) and the Surveillance Camera Commissioner (SCC), that ensure the need for public protection is balanced with respect for the privacy of individuals.

The Data Protection Act 1998 applies because the cameras will capture personal information that could identify individuals. The Council's Data Protection Policy gives more detail on how the council processes and looks after personal data.

## 2. Scope

This policy applies to all overt (open) CCTV installations controlled by the council, including both internal and external cameras and Body Worn Video (BWV) utilised by enforcement officers and employees with similar, relevant, roles. This policy also covers the use of the following types of equipment should the council decide, at any point, to utilise this technology.

- Automatic number plate recognition (ANPR)
- Unmanned aerial systems (UAS)

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

## 3. Policy Statement

The purpose of this policy aims to:

- Ensure compliance with relevant legislation, as listed in the below section.
- Ensure adherence to the ICO CCTV Code of Practice and the SCC CCTV Code of Practice.

## 4. Relevant Legislation

The council must comply with all the relevant statutory legislation, in particular the following, with regards to the installation and operation of CCTV & BWV Systems:

- Data Protection Act 1998
- 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).

## 5. Duties and Responsibilities

Leicestershire County Council is registered as a Data Controller under the Data Protection Act (1998) and has responsibility for the fair and lawful processing of personal and/or sensitive personal information rests with the Chief Executive on behalf of the Council as a whole.

CCTV and BWV are services which inherently fall into the scope of the Data Protection Act 1998 due to amount of personal data that is captured by the cameras.

If your role at Leicestershire County Council includes CCTV or BWV either as a direct responsibility or peripheral to your normal tasks, this policy is relevant to you. As an individual representing or working for the Council it is essential that you understand and abide by the following:

- Compliance with the Data Protection Act 1998 and the Council's Data Protection Policy, where relevant, for the operation of CCTV & BWV systems.
- Appropriate level of operational knowledge and training for CCTV & BWV operators.
- CCTV & BWV Operators to complete the Data Protection & Information Security eLearning as a minimum training level.
- Corporate and/or departmental policy, procedures and guidance on the operation of CCTV & BWV systems are implemented and followed.
- Appropriate physical security, where required, is in place to assure the integrity of the CCTV & BWV Systems and their recordings.
- Retention periods documented and adhered with regards to CCTV & BWV footage.

- Access to footage strictly controlled to relevant and authorised personnel only.

## 6. Purpose of the CCTV system

The Council's CCTV & BWV systems are used for the following key objectives which will be subject to an annual assessment:

- To detect, prevent or reduce the incidence of crime
- To prevent and respond effectively to all forms of possible harassment and disorder.
- To reduce the fear of crime
- To create a safer environment
- To provide emergency services assistance
- To assist with health and safety and other serious occurrences, including employment issues.

## 7. Surveillance Camera Commissioner (SCC)

The Secretary of State has issued a Surveillance Camera Code of Practice under Section 30 of the Protection of Freedoms Act 2012, which provides guidance on the use of CCTV & BWV cameras. It explains how the government is supportive of the use of overt CCTV & BWV provided that certain conditions are met and to ensure these are met has put together the following twelve guiding principles.

There are more details for each of the 12 principles in the Code of Practice, which must be read in conjunction with this policy. The 12 principles, which have been adopted, in full, by the council, are;

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.

The SCC is a statutory appointment by the Home Secretary to promote compliance with the Surveillance Camera Code of Practice and to provide advice on compliance. A SCC Guide has also been created by the Secretary of State to assist organisations with compliance.

## 8. Information Commissioner's Office (ICO) CCTV Code of Practice

The ICO has produced a Data Protection Code of Practice for CCTV & BWV to assist organisations who use CCTV & BWV to comply with the Data Protection Act 1998. The ICO regulates the Data Protection Act in the UK.

The ICO Code of Practice details how CCTV & BWV can be compliant with the 8 guiding principles of the Data Protection Act 1998.

The Code gives guidance in areas such as deciding when CCTV & BWV should be used, governance of the personal data CCTV & BWV system collect, how to use the equipment and organisational responsibilities.

As with the SCC Code of Practice, the ICO Code has also been adopted, in full, by the Council.

## 9. How images and Information are stored.

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

Recorded images and CCTV & BWV information will only be used for the purposes defined in this Policy and in both the ICO and SCC Codes of Practice and ownership of the recorded material is with the council as the Data Controller. Recording equipment will be checked to a regular schedule, as defined in each Code of Practice.

CCTV & BWV images will only be viewed when there is a legitimate business 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.

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

## 10. Requests for footage

CCTV & BWV footage can be requested through various routes, predominantly the Data Protection Act 1998 or the Freedom of Information Act 2000. Inappropriate access, use or disclosure of CCTV & BWV footage may put

members of the public, employees or CCTV & BWV operators at risk of serious harm, damage or distress, the Council at risk of reputational damage and/or be a breach of the law.

### Data Protection Act 1998

Individuals who are captured on CCTV or BWV footage are entitled to request a copy of that footage. There are various ways under the Data Protection Act in which footage can be requested, the most common of which are listed below. For further information on these request types please read the council's Data Protection Policy which details the circumstances in which each request can be made, by whom and the process for dealing with them.

- Subject Access Requests
- Section 35 Requests (S35)
- Section 29 Requests (S29)

### Freedom of Information Act 2000 (FoIA)

CCTV & BWV images can be requested under the Freedom of Information Act 2000. FoIA deals with information the council holds, but personal information is usually exempt under S40 of the Act. However there may be instances where footage does not contain personal information and as such will need to be considered for release. Each request made under FoIA for CCTV & BWV images must be responded under the normal Freedom of Information process.

### Internal Requests for Information

Sometimes internal departments may need to request access to CCTV & BWV images in connection with internal investigations. Any requests of this type need to be made in writing to the CCTV or BWV Operator and approved by Policy & Assurance and signed off by the relevant director.

## 11. 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 CCTV footage is not considered to be covert recording and is therefore covered by this policy and outside of the RIPA process. This is due to the camera being in plain sight for individuals to see and appropriate

signage as per the Codes of Practice from the ICO & SCC. If a decision is made to monitor a particular employee, or member of the public, this is considered to be targeted surveillance, which falls under RIPA (Regulation of Investigatory Powers Act 2000).

Moving or zooming CCTV towards individuals and their activities would be considered covert surveillance and fall outside of this policy and into RIPA unless criminal activity or public safety issues are already taking place, and cameras are moved or zoomed in response to this.

Body Worn Video is not appropriate for Covert use, as it requires placement on an individual, in plain sight to work and as such cannot, in almost all cases, be covert, unless the equipment has been purchased with covert work in mind. However, should the council in the future decide to purchase smaller, more covert BWV, then the above section on covert surveillance could be appropriate.

## 12. Policy Review

A review of this policy will take place every two years or as required to take account of any new or changed legislation or regulations of business practices.

## 13. Breaches of this Policy

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 Policy and Assurance Team.

Actions or neglect leading to a breach of this policy, or failure to report a breach will be investigated.

## 14. 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. 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.