



Video Surveillance System Policy

Version number: 1
December 2023

Tracking

Revision History

1. Initial document for Committee

Document Approvals

Adopted by the Council on 12 December 2023 (item 34)

Each revision requires the following approvals:

- Non-administrative updates: SLT followed by relevant Committee
- Administrative updates: Head of Policy and Corporate Resources.

Introduction

There is a responsibility under Section 17 of the Crime and Disorder Act 1998 for local authorities to consider crime and disorder reduction while exercising their duties. The Council is committed to improving community safety and to protect the Council's assets. CCTV cameras are used by Epsom & Ewell Borough Council in the town centre, on vehicles, in other public areas and in/on buildings/assets where the Council has a legitimate interest.

Organisation description

Epsom & Ewell Borough Council ("the Council"), is a local government district with borough status and unparished area in Surrey, England, covering the towns of Epsom and Ewell and surrounding areas.

Policy Statement

This policy sets out how the Council will operate and maintain Video Surveillance Systems (VSS), across the Borough. It sets out the criteria and standards for the maintenance, upgrading and replacement of VSS and the rationale for the purpose of the positioning and installation of any new cameras and supporting surveillance technology.

The Council will respect people's right to privacy and ensure the use of Video Surveillance Systems is regulated to ensure consistency and compliance with legislation, standards and best practice.

Video Surveillance Systems (VSS) definition

Video Surveillance Systems has the meaning given by Section 29(6) of the Protection of Freedoms Act 2012 and is taken to include:

(a) closed circuit television (CCTV) or automatic number plate recognition (ANPR) systems.

(b) any other systems for recording or viewing visual images for surveillance purposes.

(c) any systems for storing, receiving, transmitting, processing or checking the images or information obtained by (a) or (b);

(d) any other systems associated with, or otherwise connected with (a), (b) or (c)

Generally, this will include conventional CCTV, any Automatic Number Plate Recognition (ANPR), body worn cameras, vehicle installed cameras and mobile or re-deployable systems. It also includes any AI (artificial Intelligence) systems related to the above (includes automatic face recognition systems), and the use of Drones (UAV - unmanned aerial vehicles).

In a very few occasions, audio recording may be incorporated into Video Surveillance Systems.

Policy Rationale

This Policy affects everyone who lives, works and visits the Borough so it is essential that the Council has a policy that reflects the uses of Video Surveillance Systems in a manner that complies with the law and continues to receive public support and confidence.

This Policy applies to all staff employed by Epsom & Ewell Borough Council and provides the standard expected from any external agencies or persons who operate Video Surveillance Systems on the Council's behalf.

The Video Surveillance Systems are operated and maintained by Epsom & Ewell Borough Council and are operated to the requirements of the General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 ("DPA") and good practice guidelines, such as those issued by the Information Commissioner's Office (ICO), to ensure, for example that the need for public protection is balanced with respect for the privacy of individuals.

GDPR applies because Video Surveillance Systems capture personal information that could identify a living individual. This policy outlines the principles the Council adheres to, the processes that the Council follows and related policies and processes, such as those regarding how to request information including CCTV images.

The Council's Code of Practice related to the use of Video Surveillance Systems are informed by this policy. A separate Code of Practice is compiled to support each type of Video Surveillance System deployed.

Policy Scope

This policy applies to all overt Video Surveillance Systems controlled by the Council. This includes both internal and external cameras. All Video Surveillance Systems will be controlled by authorised members of staff trained in the operation of the system and the rules and procedures relating to its operation.

This policy does not apply to the covert use of video surveillance tools that is covered by the Council's Regulation of Investigatory Powers (RIPA) Policy. This policy does not cover the use of licensee/resident/Tenant/Leaseholder owned CCTV on residential or commercial Council property

Any use of covert video surveillance systems monitoring will be undertaken in accordance with the requirements set out in the Regulation of Investigatory Powers Act 2000 (RIPA). RIPA requires that due consideration is given to the proportionality and necessity of any covert activity and that regard is given to the rights of individuals under Article 8 of the Human Rights Act (the right to privacy).

Details of key personnel

- Head of Housing and Community for town centre, mobile and body worn schemes

- Head of Property and Regeneration for building asset schemes
- Head of Operational Services for vehicle and parks based schemes
- Head of Legal and Democratic Services as Senior Responsible Officer (SRO)
- Data Protection Officer (DPO)

Each person may nominate a suitably qualified deputy for day-to-day operational matters

Relevant Police force

Surrey Police - Margaret Road, Guildford, Surrey, GU1 4QS

Key Personnel - CCTV Change Manager & Contact Duties Manager

Video Surveillance System Objectives and Legitimate Aims

The objectives of the use of Video Surveillance Systems are

- To reduce the fear of crime
- To deter crime, detect crime and provide evidence of offences
- To enhance community safety, assist in developing the economic wellbeing of Epsom & Ewell and encourage greater use of the facilities and amenities of the Borough
- To assist the Council in its enforcement and regulatory functions
- To support civil proceedings
- To assist with meeting the Council's obligations for staff and contractor safety
- To assist the Council to deliver its statutory and other functions
- To assist in the management of Council premises and contracts
- To assist the Council in its overall resilience planning linked to civil contingency planning, emergency response, counter terrorism and business continuity functions
- To assist in staff disciplinary, grievance, formal complaints and Health and Safety Investigations
- To assist the Council in meeting its obligations for the management of assets, buildings, parks, leisure facilities and other open spaces
- Assisting with the location of missing persons. This will be carried out under the General Data Protection Regulation under the category of "vital interests" which is described as the processing of information necessary to protect someone's life.

Legal Basis – 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.

In most circumstances for the use of video surveillance systems in public spaces is where it is necessary for the Council to perform a task in the public interest or for Council's official functions and the task or function which is required to have a clear basis in law. i.e. :

- Processing is necessary for compliance with a legal obligation to which the data controller is subject.
- Processing is necessary to protect the vital interests of the data subject or another person.
- Processing is necessary for the performance of a task carried out in the public interest.

To process special category data (which is undertaken with the use of Video Surveillance Systems) the following lawful conditions of Article 9 GDPR have been identified:

- 9(2)(a) Explicit consent
- 9(2)(b) The obligations of employment, social security and social protection (if authorised by law)
- 9(2)(f) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- 9(2)(g) Processing is necessary for reasons of substantial public interest (with a basis in law).
- 9(2)(i) Processing is necessary for reasons of public interest in the area of public health (with a basis in law).

Any use of covert CCTV monitoring will be undertaken in accordance with the requirements set out in the Regulation of Investigatory Powers Act 2000 (RIPA). RIPA requires that due consideration is given to the proportionality and necessity of any covert activity and that regard is given to the rights of individuals under Article 8 of the Human Rights Act (the right to privacy).

Privacy statement

Epsom & Ewell Borough Council is committed to protecting your privacy when you use our services. The Council is a data controller.

As the data controller, we must:

- Only keep your data that we need to provide services and do what the law says we must.
- Keep your data safe and accurate.
- Only keep your data as long as we have to.
- Collect, store and use your data in a way that does not break any data protection laws.

Copyright, Data Protection and GDPR

Under the General Data Protection Regulation (GDPR), we are required to publish information about what data we collect, why we need to store it, and your rights under the GDPR legislation.

In these matters we are subject to the rulings of the Information Commissioner's Office (ICO), the UK's independent authority set up to uphold information rights and data privacy for individuals.

The Council has adopted a Data Protection Policy. This document sets out our policy regarding data protection. The Data Protection Act 2018 and the General Data Protection Regulation 2016/679 form the background to the document. The Policy is drafted using the terms of the Data Protection Act 2018, the Freedom of Information Act 2000 and the Human Rights Act 1998. A copy of the policy is available on the Council's web site.

The Data Protection Act 2018 is designed to protect personal data about living individuals (Data Subjects). The Act also places obligations on those organisations that process personal data (Data Controllers). The data controller is the person who (either alone or jointly or in common with other persons) determines the purpose for which and the manner in which any personal data are, or are to be, processed.

For the purposes of this policy, Epsom & Ewell Borough Council is the data controller. We have a Data Protection Officer who makes sure we respect your rights and follow the law. If you have any concerns or questions about how we look after your personal information, please contact the Data Protection Officer, at foidpa@epsom-ewell.gov.uk or by calling 01372 732000 and asking to speak to the Data Protection Officer.

There are two types of data under the 2018 General Data Protection Regulations: "Personal data" which means any information relating to a living individual who can be identified from that information (a "data subject") on its own or when taken together with other information. This may include both facts and expressions of opinion about the person and an indication of the intentions of the Council or others in respect of that person. It does not include anonymised data.

"Special category data" which means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data. Images collected by the Council's Video Surveillance Systems will normally fall under the "Personal data" category.

For each type of Video Surveillance System, a Data Protection Impact Assessment (DPIA) is compiled.

A DPIA is a separate process from compliance checking or data protection audit processes, (an audit that is undertaken on systems that have already been implemented). The DPIA will highlight that privacy undertakings and/or privacy law are being complied with or will highlight problems that need to be addressed. All video images, audio recordings, meta data and documentation supporting the design, implementation operation and management of video surveillance systems is

the Copyright of Epsom & Ewell Borough Council, unless otherwise stated, under Section 17 of the Copyright, Designs and Patents Act 1988.

Cyber security policy and arrangements

The design, implementation, operation and maintenance of deployed Video Surveillance Systems will at all times comply with the current Council's Cyber Security Policy, the IT and Acceptable Use Policy, relevant standards and best practice.

Principles of data protection by design and default shall apply.

Accountability and Transparency

Subject Access Requests

You have the right to ask for all the information we have about you and the services you receive from us. When we receive a request from you, we must give you access to everything we've recorded about you.

However, we can't let you see any parts of your record which contain:

- Confidential information about other people; or
- Data a professional thinks will cause serious harm to your or someone else's physical or mental wellbeing; or
- If we think that giving you the information may stop us or another agency from preventing or detecting a crime.

You can make a subject access request by completing and returning the form available on the Council's web site.

Freedom of Information

All requests for information under the Freedom of Information Act 2000 should be in writing and must include your name and an address for the response. This can be sent either by post to the address below, emailed to foidpa@epsom-ewell.gov.uk or by using the FOI request form available on the Council's web site.

Please provide a description of the information that you are seeking from the Council. It may be helpful to provide a contact number as well in case we need to contact you about your request.

Address for postal correspondence: Epsom & Ewell Borough Council, Town Hall, The Parade, Epsom KT18 5BY

Our Freedom of Information Policy can be found on the Council's website.

Complaints

The Council has a published Complaints Policy available on the website at www.epsom-ewell.gov.uk. If you wish to complain about a service, express an opinion on services or policy, give praise or make a suggestion, you are able to do this by email, correspondence, in electronic format or in person if you wish at the Town Hall.

Provision of Public Information

Details of the current Video Surveillance System Policy will be published on the Council's website.

Factual information on the details of Video Surveillance Systems utilised, statistical findings of their effectiveness and review will form part of the evaluation process and be published periodically.

Access to Video Surveillance Systems

Live or recorded data from deployed Video Surveillance Systems may be viewed and/or supplied to the Police or other law enforcement agencies.

At no time shall the images supplied to the Police or other law enforcement agency be used for anything other than the purpose specified and identified when the images were released.

The responsibility for the image's safekeeping and integrity of the data will transfer to the Police or other law enforcement agency once supplied by the Council utilising the provisions of the Surrey Multi Agency Information Sharing Protocol (MAISP), and recorded by an established audit trail.

The Council will not routinely store copies of recorded data where there is no need. Where imagery is required for compliance reasons, it will be held securely and deleted as soon as it is no longer required. Only in exceptional cases of serious incidents will this be considered, and the retention must be approved by the CCTV SRO.

Any requests from members of the general public or a third party will be dealt with under the existing provisions for access via the Data Protection Act 2018, GDPR or the Freedom of Information Act 2000 processes. Prior to release the imagery will be screened for collateral intrusion and it may be necessary to restrict and/or redact imagery so as not to reveal the personal details of any other person.

The Council will not release any images, either directly or indirectly, to any organisation for inclusion in any television or other media production without explicit authority from the Chief Executive. Such circumstances might be where publicising the footage would help amplify a message such as anti-flytipping. Any unauthorised release of VSS data will be considered under the Council's disciplinary procedure.

Recorded Image and Data Retention Duration

We will only hold your personal information for as long as necessary for business purposes or if we are required to keep it by law. There's often a legal reason for keeping your personal information for a set period of time, and we try to include all of these in our retention schedule.

The detailed requirements for recording duration are outlined in the relevant Council Video Surveillance System Code of Practice.

Video Surveillance System Review

The Council has adopted operating procedures to ensure that legal requirements, policies and standards are complied with in practice and that regular reporting is published.

The detailed requirements for review are outlined in the relevant Council Video Surveillance System Code of Practice.

Management of Video Surveillance Systems

1. Asset lists

To ensure full visibility of system performance, details of each Video Surveillance System will be recorded on asset lists to enable system managers to undertake the required periodic system reviews.

2. Maintenance arrangements

Effective and regular maintenance of a CCTV system is essential to ensure that the system is effective at all times, downtime minimised by monitoring performance and software systems maintained to meet cyber security requirements.

3. Review and Audit

The Council will complete the Surveillance Camera Commissioner's Self-Assessment tool on a regular basis for all uses of Video Surveillance Systems which will confirm compliance with the twelve guiding principles of the Surveillance Camera Code of Practice in conjunction with the Council's own Code of Practice for the operation of the same.

- There is still a legitimate reason to maintain the Video Surveillance System.
- The CCTV cameras continue to provide images of sufficient quality.
- Signage remains up to date and relevant.

Periodic system reviews are undertaken to provide information for the published annual report on Video Surveillance System performance.

Applicable Legislation and Standards

- Epsom & Ewell Borough Council - Video Surveillance System Policy 2023

- Epsom & Ewell Borough Council - Video Surveillance System Code of Practice
- Data Protection Act 2018 (DPA)
- The Human Rights Act 1998 (HRA)
- The Freedom of Information Act 2000 (FOIA)
- Regulation of Investigatory Powers Act 2000 (RIPA)
- UK General Data Protection Regulation (UK GDPR)
- Crime and Disorder Act 1998
- Private Security Industry Act 2001
- Biometrics & Surveillance Camera Commissioner's Code of Practice (see Appendix One)
- Equality Act 2010
- BS EN 62676 series of standards
- UK Government – published requirements for video evidence (DSTL/NPCC)

Appendix One

Biometrics & Surveillance Camera Commissioner's Code of Practice

1. The Council, as a relevant authority defined by the Protection of Freedoms Act 2012, is required to show due regard to the Biometric & Surveillance Camera Commissioner's Surveillance Camera Code of Practice issued by the Secretary of State in June 2013.
2. 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.
3. 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.
4. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point of access to information and complaints.
5. There must be clear responsibility and accountability for all surveillance system activities including images and information collected, held and used.
6. 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.
7. 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 deleted once their purposes have been discharged.
8. 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
9. Surveillance camera 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.
10. Surveillance camera systems images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
11. There must be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports published.
12. 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 of evidential use.

13. 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.