East Herts District Council

Surveillance Technologies Policy

Document Control

Organisation	East Hertfordshire District Council
Title	Surveillance Technologies Policy
Author – name and title	Tyron Suddes – Information Governance and Data Protection Manager
Owner – name and title	Tyron Suddes – Information Governance and Data Protection Manager
Date	September 2022
Approvals	Executive
Version	1.0
Next Review Date	September 2023

Contents

1. Introduction

East Hertfordshire District Council (the Council) operates and manages a number of surveillance technologies.

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

- **Parking service and off street car parks**
- **Monitoring and/or witnessing statutory nuisances**
- **Monitoring and/or witnessing suspected environmental crimes**
- **Monitoring Council Offices**
- **Monitoring Council owned premises, including hostel sites**
- **Monitoring Launchpad premises**

All systems operate within the requirements of the Data Protection legislation (noted in section 5 below) and good practice guidelines, such as those issued by the Information Commissioner's Office (ICO) and the Surveillance Camera Commissioner (SCC). The ICO code provides good practice advice for those involved in operating surveillance technologies, including how organisations can meet their data protection obligations when using these devices. The aim of the SCC code is to ensure that surveillance 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.

2. Scope

This policy applies to all overt surveillance (including audio) technologies controlled by the Council and utilised by 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, the provisions of this policy will apply. The Council will consider whether this policy requires amendments to take into account new technology.

If applicable, only sections 6-8 and 10 of this policy will apply to the use of RIPA authorised surveillance to set out how this type of surveillance data will be managed. RIPA authorised surveillance is generally governed by Regulation of Investigatory Powers Act (RIPA) 2000 Policy.

3. Policy Statement

The purpose of this policy is to:

- ensure compliance with relevant legislation, as listed in Section 5;
- ensure adherence to the Surveillance Camera Code of Practice (Section 30 of the Protection of Freedoms Act 2012) and particularly the 12 principles set out in this code as listed in appendix 1;
- 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 Technologies

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

These technologies include the following:

- Fixed CCTV - static (including, pan, tilt and zoom) cameras, which may transmit images to a control, monitoring and/or recording facility, including cameras activated by motion;
- Body Worn Cameras - Cameras worn on person which may transmit images to a control, monitoring and/or recording facility;
- Surveillance technologies that also include audio recording.

A full list of the Council's current surveillance technology use is noted in Appendix 2 – Surveillance Asset Register.

5. Relevant Legislation

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

- Data Protection Act 2018
- The retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the "UK GDPR"),
- Human Rights Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Protection of Freedoms Act 2012
- Regulation of Investigatory Powers Act 2000
- Private Security Industry Act 2001 Of Practice 2013

6. Roles and Responsibilities

The Council is a Data Controller under data protection legislation and has responsibility for the fair and lawful processing of personal data.

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

If a staff role includes the use of surveillance systems, either as a direct responsibility or peripheral to normal tasks, the employee may only use surveillance systems as determined in this policy. It is essential that all Council staff understand and abide by the following appropriate responsibilities:

6.1. Service Manager Responsibilities

This section is aimed at service managers that operate and/or oversee surveillance systems and/or are looking to procure new systems within their service.

Service Managers have the following responsibilities:

- Working with the Information Governance and Data Protection Manager:
    - to complete a Data Protection Impact Assessment;
    - to ensure that Privacy Notices are up to date and, where required, implemented.
- 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 system in accordance with the SCCP.

- Regular updating of 'local' system operating procedures.
- Ensuring that appropriate physical security is in place to assure the integrity of the surveillance system 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 read, understand, and abide by this Policy.
- Identifying and implementing specific training for staff working with surveillance 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 Surveillance Asset Register for new systems and maintaining the quality of information linked to 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 systems and must:

- Comply with this policy and other Council data protection policies, and any other relevant documentation when operating surveillance systems.
- Have an appropriate level of operational knowledge and training in the control, use and management of the surveillance devices.
- Undertake and complete any specific training linked to their duties and the surveillance technology being used.
- Ensure that the surveillance devices are working on a day-to-day basis.
- Bring defective equipment issues to the attention of their line 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 to use surveillance technology has identified a specific purpose in line with the relevant legislation for doing so.
- Support appropriate processes when requests for footage are received – see section 9.

6.3. Information Governance and Data Protection Manager Responsibilities

The Information Governance and Data Protection Manager has the following responsibilities regarding surveillance technologies:

- Supporting services in the completion and approval of Data Protection Impact Assessments.
- Ensuring policy documentation related to overt surveillance and data protection legislation is up to date.
- Coordinating / investigating information incidents linked to surveillance systems.
- Supporting data subject right requests relating to surveillance recordings.

7. Storage and Security

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

Recordings will be stored securely in digital format. Where there is a legitimate reason to keep recordings longer than the usual retention period, these 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.

Recordings and associated information will only be used for the purposes defined for each system. These 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 relevant legislation.

8. Retention

Recordings that are not required for the purpose(s) for which the surveillance system is being used will not be retained for longer than is necessary and in any event any recording will not be kept for longer than the period noted in the Council's Retention Schedule.

Access to and security of recordings will be controlled in accordance with the requirements of data protection legislation. Relevant security measures will be implemented to prevent unauthorised access to, alteration, disclosure, accidental loss or destruction of recorded material.

9. Access Requests

Council services, individual staff members, or members of the public may request access to 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 system must be able to recognise a request for access to recordings 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 Access to Information Policy.

Requests by external organisations for recordings containing personal data may be permitted under Schedules 2 -4 of the Data Protection Act 2018 but careful consideration needs to be given to whether disclosure is necessary and proportionate.

Recordings can be requested under the Freedom of Information Act 2000 (FOI) and/or the Environmental Information Regulations 2004 (EIR). Personal information is exempt from disclosure but there may be instances where footage does not contain personal information and will need to be considered for release. Requests made under FOI and/or EIR must be handled in accordance with the Access to Information Policy.

10. Regulation of Investigatory Powers (RIPA)

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.

If the use of directed surveillance is authorised under RIPA, such surveillance will be governed and safeguarded using the roles, responsibilities and procedures noted in sections 6 to 8 above. Any personal data captured during the recording of RIPA authorised surveillance will be governed in line with the Council's Data Protection Policy.

RIPA authorised surveillance will only be retained for only as long as is required

for the prevention or detection of criminal offences and any associated investigations or proceedings. The retention and disposal of RIPA authorised surveillance will be carried out in line with the Council's Data Retention Policy and the relevant retention period will be noted in the Council's Retention Schedule so that it can be regularly reviewed. Any RIPA authorised surveillance technologies will be recorded in the Council's Surveillance Asset Register.

11. Hertfordshire CCTV Partnership

East Hertfordshire District Council is a main partner of the Hertfordshire CCTV partnership which is a joint initiative aimed at reducing the fear of crime across the principal public, residential, retail, business and schools within the partnership. This policy does not govern the use of surveillance systems within the partnership; this is instead governed by the partnership's code of practice. Surveillance assets that form part of the partnership that may be used by the Council are noted in Appendix 2 below.

12. Breaches of this Policy

Inappropriate access, use or disclosure of recordings may put members of the public, employees or 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 recordings will be strictly controlled, and any breaches of this policy or operational guidance will be investigated.

All breaches and suspected breaches of this policy must be reported to your line manager.

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 in line with the Code of Conduct for Employees.

Appendix 1 – Surveillance Code of Practice

The Council's use of surveillance technologies must always comply with the 12 principles set out in the **Surveillance Code of Practice**:

1. Use of a surveillance 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 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 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 system activities including images and information collected, held, and used.

5. Clear rules, policies and procedures must be in place before a surveillance 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 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 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 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 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 system which compares against a reference database for matching purposes should be accurate and kept up to date.

Appendix 2 – Surveillance Asset Register

This register records the location and scope of Council surveillance systems and the steps taken to mitigate risks particular to each location.

Location Type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
Hertford Town Centre	Fixed CCTV	Hertfordshire CCTV Partnership public space CCTV coverage	Pre-set tours and operators	24 Hour Police airwaves Town Centre link radios CCTV Operators	Hertfordshire CCTV Partnership Code of Practice
Bishop's Stortford Town Centre	Fixed CCTV	Hertfordshire CCTV Partnership public space CCTV coverage	Pre-set tours and operators	24 Hour Police airwaves Town Centre link radios CCTV Operators	Hertfordshire CCTV Partnership Code of Practice
Ware Town Centre	Fixed CCTV	Hertfordshire CCTV Partnership public space CCTV	Pre-set tours and operators	24 Hour Police airwaves Town Centre link	Hertfordshire CCTV Partnership Code of Practice

Location Type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
		coverage		radios CCTV Operators	
Stanstead Abbotts	Fixed CCTV	Hertfordshire CCTV Partnership public space CCTV coverage	Pre-set tours and operators	24 Hour Police airwaves Town Centre link radios CCTV Operators	Hertfordshire CCTV Partnership Code of Practice
Varying locations across East Herts District. Installed into properties as needed to monitor and/or witness statutory	Noise recording equipment	4	Varies depending on the nature of the nuisance.	All recordings will be reviewed.	The subject of a nuisance complaint is informed that we are investigating and noise recording equipment may be used to determine whether a statutory nuisance is likely to exist or not. Devices are

Location Type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
nuisances					generally controlled by the person being disturbed by the nuisance, though they can be used on a timer basis if needed.
Wallfields	Fixed CCTV	38	24hrs	During staffed office hours	Wallfields is signed with appropriate signage for CCTV, its use and purpose with contact details
Charringtons EHDC Office	Fixed CCTV	10	24hrs	During staffed office hours	Charringtons is signed with appropriate signage for CCTV, its use and purpose with contact details
Charringtons	Fixed CCTV	6	24hrs	During staffed	Buntingford is

Location Type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
Common Parts				office hours	signed with appropriate signage for CCTV, its use and purpose with contact details
Buntingford Service Centre (New)	Fixed CCTV	12	24 hrs	24hrs (Herts CCTV partnership)	Buntingford is signed with appropriate signage for CCTV, its use and purpose with contact details
Buntingford Service Centre (Old)	Fixed CCTV	10	24hrs	During Staffed Office Hours	Buntingford is signed with appropriate signage for CCTV, its use and purpose with contact details

Location Type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
Launchpad Charringtons house	Fixed CCTV	6 (5 of ground floor, 1 of 2nd floor south)	24hrs, (retained for 10 days)	Ad-hoc. 3 people have access if/when required. (2 x LP staff and maintenance	Launchpad facility is open 24/7 - accessible with key-fob. No alarm. There is valuable equipment in the office belonging to members. The CCTV is necessary for security for both persons and belongings. Reassuring for lone workers. CCTV signage shown in entrance lobby

Location Type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
The Rectory & Cedar Hostels	Fixed CCTV	21	24 hrs (only records motion so retention of recordings depends on motion, however, generally recordings are not kept for more than 28 days)	Mon-Fri 9-5 Remote access via staff mobile phones	Low level; All residents are advised on move-in that CCTV is in operation in communal areas and sign a letter to confirm that they have been informed of this. Signage in communal areas
Hillcrest Hostel	Fixed CCTV	6	24 hrs	Staff working hours 10-2 Mon-Fri	Low level; Signage in car park
Varying locations - Licensing and	Bodycams	4	Activated by officer when an offence is suspected	Following surveillance if offence is suspected. Any	Officers will be trained on how to use and operate the devices

Location Type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
Enforcement Bodycams				surveillance not linked to an offence will be deleted	Service Manager to make a decision about whether surveillance can be used Surveillance to be carried overtly by constantly notifying persons of ongoing recording Intrusion of individuals' privacy rights to be reduced by only recording when proportionate and necessary in line with legislation

Location Type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
Varying locations - Licensing and Enforcement Radios	Radios	3	Activated by officer when an offence is suspected	Following surveillance if offence is suspected. Any surveillance not linked to an offence will be deleted	Officers will be trained on how to use and operate the devices Service Manager to make a decision about whether surveillance can be used Surveillance to be carried overtly by constantly notifying persons of ongoing recording Intrusion of individuals' privacy rights to be reduced by only recording when proportionate

Location Type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
					and necessary in line with legislation
Varying locations – Licensing and Enforcement Wildlife Cameras	Mobile cameras	7	24hrs (cameras relocated every 10 days)	Following surveillance if offence is suspected. Any surveillance not linked to an offence will be deleted	Cameras to be suitably camouflaged to avoid theft. Cameras to be frequently relocated (every 10 days maximum). Cameras not to be placed in areas of high foot fall or vehicle traffic Cameras to be removed upon positive identification of a

Location Type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
					subject for prosecution. Cameras to have suitable signs linking to privacy information