eastsussex.gov.uk

East Sussex
County Council

Surveillance Camera Policy

December 2017

V0.3

eastsussex.gov.uk

East Sussex County Council

Surveillance Camera Policy

Summary

This policy describes what the organisation must have in place in order to deploy the use of overt surveillance technology.

Contents

This document forms part of a suite of Information Management Policy and Guidance, details of which can be found on the intranet.

Change must be agreed by the Senior Information Risk Officer (SIRO).

Document Approved By:	
Approval date	
Review date:	
Security Classification:	Official - Disclosable

Surveillance Camera Policy

1. Overview

This policy describes ESCCs obligations with regard to monitoring in public spaces and Council property and the associated use of surveillance camera technology

This policy exists to:

- ensure compliance with relevant law and codes of practice
- safeguard personal data collected and stored by the council

2. Scope

This policy applies to delivery of services by all functions within the council.

3. Definitions

'Surveillance technology' is defined in this context as any 'systems used to monitor or record the activities of individuals, or both' (ICO Surveillance Camera Code of Practice (2015)). These include:

- Closed Circuit Television (CCTV)(with and without audio)
- Body Worn Video (BWV)
- Unmanned aerial systems (including Drones)

Monitoring the activities of individuals using surveillance technology involves the processing of Personal Data, defined under data protection law as information that allows identification of an individual.

'Monitoring' in the context of surveillance will often mean that personal data is collected outside of the purpose for which surveillance has been implemented as opposed to direct recording of an event/meeting (subject to separate policy).

'Overt surveillance'- this policy covers monitoring where data subjects are aware of the fact that surveillance is taking place. This is distinct from covert surveillance covered under ESCC's RIPA Policy.

4. Procedure

In order to ensure the Council upholds individuals' rights in processing personal data and complies with relevant legislation, any deployment of the use of surveillance technology must be designed and risk assessed using the following process:

a. A Privacy Impact Assessment and Surveillance Checklist (see Appendix 1) must be completed and signed off for each use and deployment* of surveillance technology.

b. A technical Risk Assessment must be completed and signed off for each use and deployment of surveillance technology

*Deployment refers to a common instance of Surveillance Camera Technology i.e. using the same

technology and processes for the same purpose and can therefore cover more than one camera.

5. Use of data gathered via the use of surveillance technology

The use of data gathered via surveillance technology must be clearly articulated, justified and documented in the Privacy Impact Assessment (see section4).

Data must only be held for as long as is required to meet the purpose for which it was gathered unless a legal exemption applies. Requests by individuals for data be erased must be considered in line with Data Protection Law (see section 6).

6. Data Subject Rights

Individuals whose personal data has been collected via the use of surveillance technology have a right to access and/or obtain a copy of this data and to exercise any other relevant right under Data Protection Law (unless an exemption applies).

To exercise data subject rights e.g. right of access, erasure, rectification etc, individuals can make requests via the ESCC Website and/or the Customer Services Team.

7. Related Policies, Guidance and Legislation

General Data Protection Regulation/Data Protection Act
Regulation of Investigatory Powers Act
Protection of Freedoms Act
Human Rights Act

ESCC Information Security Policy
RIPA Policy

Home Office, Surveillance Camera Code of Practice
ICO, CCTV Code of Practice

Appendix 1

Surveillance Checklist

Privacy Impact

☐ Is there a clear and legitimate purpose for use of surveillance? E.g. detection and prevention of crime
☐ Are there no alternatives to use of surveillance? Is there a pressing need for the use of surveillance technology?
☐ Is the processing lawful? (Does an applicable condition to process apply?)
☐ Will a robust privacy notice/signage be in place outlining the existence of surveillance and the use of personal data? (See PN guidance/checklist)
☐ Is personal data collected only to be used for the purposes outlined?
☐ Is only the minimum data required to fulfil the purpose collected?
☐ If applicable, is recording of audio data suitably justified? Has a 'pressing need' for audio been clearly articulated? Is there no other alternative?
☐ Has a Data Privacy Impact Assessment (DPIA) been completed and this checklist appended?

Security

☐ Is security of images assured from capture to destruction?
☐ Is access to view data confined to a secure area/office?
☐ Has the solution to be used been risk assessed (by IT&D)?
☐ Are all operator staff security cleared?

Procedure and Governance

☐ Are robust procedures in place to ensure authorised access only?
☐ Is a contract in place with any 3rd party supplier that assures compliance with data protection law?
☐ Do procedures clearly outline who, how and when personal data should be accessed, stored and disclosed?
☐ Are all operator staff trained in relevant procedures including access, disclosure (inc. subject access) and retention?
☐ Are staff aware of the consequences of the misuse of surveillance technology?
☐ Will the use of surveillance be reviewed annually?
☐ Is there an Information Asset Owner identified?
☐ Is information kept only for as long as required to fulfil the purpose for processing?
☐ Is the operator of the surveillance technology suitably licenced?
☐ Can surveillance be 'turned off' when not required?
☐ Can data subject rights be met e.g. erasure?

Technical

 Is the accuracy and integrity of information assured? Does image quality and metadata (e.g. date and time) meet requirements for processing the data?
 Can images be pixelated for disclosure/subject access purposes?
 Do systems allow ease of disclosure where relevant?
 Is an audit of access and disclosure to be kept?
 Can data be made available in a commonly used format?
 Does positioning of cameras/surveillance equipment exclude areas where individuals would have a legitimate expectation of privacy?
 Do disclosure mechanisms allow secure delivery to intended recipients?
 Where both audio and visual recording is in place, can these be enabled independently e.g. can audio be switched on and off?