



## LEAD MEMBER FOR COMMUNITIES AND SAFETY

**DECISIONS** to be made by the Lead Member for Communities and Safety,  
Councillor Bill Bentley

**TUESDAY, 27 FEBRUARY 2018 AT 10.00 AM**

**CC2 - COUNTY HALL, LEWES**

### **AGENDA**

- 1 Decisions made by the Lead Cabinet Member on 25 January 2018 (*Pages 3 - 4*)
- 2 Disclosure of Interests  
Disclosure by all Members present of personal interests in matters on the agenda, the nature of any interest and whether the Members regard the interest as prejudicial under the terms of the Code of Conduct.
- 3 Urgent items  
Notification of any items which the Lead Member considers urgent and proposes to take at the appropriate part of the agenda.
- 4 Surveillance Camera Policy (*Pages 5 - 12*)  
Report by the Chief Operating Officer
- 5 Any urgent items previously notified under agenda item 3

PHILIP BAKER  
Assistant Chief Executive  
County Hall, St Anne's Crescent  
LEWES BN7 1UE

19 February 2018

Contact Simon Bailey, Democratic Services Officer,  
01273 481935  
Email: [simon.bailey@eastsussex.gov.uk](mailto:simon.bailey@eastsussex.gov.uk)

This page is intentionally left blank

## LEAD MEMBER FOR COMMUNITIES AND SAFETY

DECISIONS made by the Lead Member for Communities and Safety, Councillor Bill Bentley, on 25 January 2018 at County Hall, Lewes

---

### 20 DECISIONS MADE BY THE LEAD CABINET MEMBER ON 27 SEPTEMBER 2017

20.1 The Lead Member confirmed as a correct record the minutes of the meeting held on 27 September 2017.

### 21 DISCLOSURE OF INTERESTS

21.1 There were no disclosures of interest.

### 22 URGENT ITEMS

22.1 There were no urgent items.

### 23 REGISTRATION SERVICE - PROVISION OF DISCRETIONARY SERVICES

23.1 The Lead Member considered a report by the Director of Communities, Economy and Transport.

#### DECISIONS

23.2 The Lead Member RESOLVED to:

- 1) Note the breadth of discretionary services currently being pursued by the Registration Service;
- 2) Approve the implementation of a new discretionary service providing funerals and wakes at Southover Grange; and
- 3) Delegate authority to the Director of Communities, Economy and Transport to discount non-statutory ceremony fees by up to 25%.

#### REASON

23.3 There is a recent but growing trend for civil funerals to be held in venues other than a crematorium. Once the funeral ceremony has been completed the Funeral Director then accompanies the body to the crematorium and the mourners remain in situ for the wake. The benefit of this arrangement is that the funeral ceremony itself does not need to be rushed as is often the case at crematoria and the guests can stay in the same venue for the funeral and the wake afterwards. Some areas are not well covered by the crematoria available, which involves a lot of travelling for many people, and some family members prefer funerals to take place in more attractive buildings than some of the crematoria that are available. Southover Grange is an ideal venue for offering this new service.

23.4 Discounting non-statutory ceremony fees by up to 25% if they are booked at the same time as the customer is conducting other business with the Registration Service provides

opportunities for customers to, for example, book a non-statutory naming ceremony while in the office to register the birth of a baby.

23.5 The Lead Member thanked staff for helping to develop the number of new discretionary services currently being pursued by the Registration Service. He encouraged staff to continue to come forward with additional ideas and assured them that he would help to promote these ideas where possible.

Report to: **Lead Cabinet Member for Communities and Safety**

Date: **27 February 2018**

By: **Chief Operating Officer**

Title of report: **Surveillance Camera Policy**

Purpose of report: **To approve the County Council's Surveillance Camera Policy**

---

**RECOMMENDATION: The Lead Member is recommended to approve the County Council's Surveillance Camera Policy**

---

## **1 Background**

1.1 The Surveillance Camera Policy is required in support of compliance with new data protection legislation and surveillance camera codes of practice produced by the Information Commissioner's Office and the Home Office)

## **2 Supporting Information**

2.1 The East Sussex County Council Policy is attached as Appendix 1 and has been approved by the Information Strategy Board and Statutory Officers Group.

2.2 The Policy describes what the organisation must have in place in order to deploy the use of overt surveillance technology.

## **3 Conclusion and reason for recommendation**

3.1 The Lead Member for Communities and Safety is recommended to approve the Policy as set out in Appendix 1, as it will ensure the Council complies with its statutory requirements.

Kevin Foster  
Chief Operating Officer

Matt Scott  
Chief Information Officer

Contact Officer: Heidi Judd Tel No: 01273 482184  
Local Member: All

This page is intentionally left blank



# Surveillance Camera Policy

December 2017

V0.3



# 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

- 1. Overview .....3
- 2. Scope .....3
- 3. Definitions.....3
- 4. Procedure.....3
- 5. Use of data gathered via the use of surveillance technology.....4
- 6. Data Subject Rights.....4
- 7. Related Policies, Guidance and Legislation .....4
- Appendix : Surveillance Checklist.....5

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).

<b>Document Approved By:</b>	
<b>Approval date</b>	
<b>Review date:</b>	
<b>Security Classification:</b>	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 section 4).

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 to 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 3<sup>rd</sup> 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?