ADUR & WORTHING
COUNCILS

Joint Governance Committee
28 November 2017
Agenda Item 9

Key Decision [Yes/No]

Wards: All

Close Circuit Television (CCTV) Policy

Report by the Director for Digital & Resources

1.0 Summary

1.1 To agree a CCTV Policy to ensure compliance with Data Protection legislation and to ensure good operational arrangements are in place.

2.0 Background

2.1 This purpose of the CCTV policy (see Appendix A) is to ensure that Adur District Council and Worthing Borough Council ("the Council") complies fully with its legal obligations under the Data Protection Act 1998 (DPA) and General Data Protection Regulation[1] (GDPR) in relation to the protection of personal data that it holds / processes about or concerning any individual. See Appendix A.

2.2 This policy adheres the good practice standards recognised by the Information Commissioner's Office and Surveillance Camera Commissioner which must be adhered to for operating CCTV. The Surveillance Camera Commissioner (SCC) was created under the Protection of Freedoms Act 2012 (POFA) to regulate CCTV and promote the CCTV code of practice and 12 guiding principles. By following these provisions the Council will ensure that arrangements are both fair and lawful.

2.3 This policy covers the use of overt cameras related surveillance equipment including

- Automatic Number Plate Recognition (ANPR)
- body worn video (BWV);

[1] GDPR comes into force 25th May 2018 superseding the DPA.

- unmanned aerial systems (UAS) aka Drones; and
- other systems that capture information of identifiable individuals or information relating to individuals.

2.4 Covert surveillance activity is not covered in the policy because this activity is governed by the Regulation of Investigatory Powers Act 2000. This type of recording is covert and directed at an individual or individuals. See the Council's' Surveillance Policy and Procedures.

3.0 Proposals

3.1 That the Joint Governance Committee, on behalf of the Councils, approves the CCTV policy.

4.0 Legal

4.1 The Surveillance Camera Commissioner (SCC) was created under the Protection of Freedoms Act 2012 (POFA) to regulate CCTV and promote the CCTV code of practice and 12 guiding principles. The processing of personal data must comply with the Data Protection Act 1998 and GPDR (from 25th May 2018).

5.0 Financial implications

5.1 There are no specific financial implications arising from this report.

6.0 Recommendation

6.1 That the Joint Governance Committee agrees the CCTV Policy as set out in Appendix 1 with immediate effect.

Local Government Act 1972
Background Papers:

Information Commissioner's Office Data Protection Code of Practice for Surveillance Cameras and Personal Information (June 2017)
Surveillance Camera Commissioner, The Surveillance Camera Code of Practice (June 2013)

Contact Officer:

Barbara Bastable
Senior Information Officer
01903 221007
barbara.bastable@adur-worthing.gov.uk

Schedule of Other Matters

1.0 Council Priority

1.1 This report does not address any particular Council priority.

2.0 Specific Action Plans

2.1 This report does not address any specific action plan.

3.0 Sustainability Issues

3.1 This matter does not address any particular sustainability issues.

4.0 Equality Issues

4.1 This matter does not address any particular sustainability issues.

5.0 Community Safety Issues (Section 17)

5.1 The Policy and Procedure set out within this report is intended to improve the appropriate and proportionate use of CCTV for detecting crime, which in itself, should help to reduce crime within the area.

6.0 Human Rights Issues

6.1 This Policy and Procedure is intended to ensure that human rights are considered prior to and during the operation of CCTV. The use of privacy impact assessments and CCTV self assessments would provide the Councils with protection to any claim that an individual's human rights have been breached.

7.0 Reputation

7.1 The Policy and Procedure is intended to ensure that the Councils act properly and proportionately when considering using CCTV and where used that appropriate arrangements are put in place. .

8.0 Consultations

8.1 Consultation has been undertaken with the Council's' Leadership Team

9.0 Risk Assessment

9. Matter considered and no issues identified.

10.0 Health & Safety Issues

10.1 Matter considered and no issues identified.

11.0 Procurement Strategy

11.1 Matter considered and no issues identified.

12.0 Partnership Working

12.1 Matter considered and no issues identified.

Appendix A

ADUR & WORTHING
COUNCILS

Close Circuit Television (CCTV) Policy

Date	Version number	Changes
28/10/17	1.0	Approved by Joint Governance Committee

This policy will be reviewed annually

1 Introduction

This policy is in place to ensure that Adur District Council and Worthing Borough Council ("the Council") complies fully with its legal obligations under the Data Protection Act 1998 (DPA) and General Data Protection Regulation[2] (GDPR) in relation to the protection of personal data that it holds / processes about or concerning any individual. See Appendix A.

2 Purpose and scope

This policy details the good practice standards recognised by the Information Commissioner's Office and Surveillance Camera Commissioner which must be adhered to for operating CCTV.

The Information Commissioner's Office (ICO) is responsible for administering the provisions of the DPA and GDPR and has powers to take legal action and fines against organisations found to be acting unlawfully.

The Surveillance Camera Commissioner (SCC) was created under the Protection of Freedoms Act 2012 (POFA) to regulate CCTV and promote the CCTV code of practice and 12 guiding principles. See Appendix B.

By following these provisions the Council will ensure that arrangements are both fair and lawful. Certain images recorded by a CCTV scheme are classed as personal data under the terms of the DPA and GDPR. The DPA and GDPR defines personal data as "data which relate to a living individual who can be identified:

a) from those data and
b) from those data and other information which is in the possession of, or is likely to come into the possession of the Data Controller.

Personal data is not limited to the ability to name an individual.

This policy document must be read in conjunction with the ICO Data Protection Code of Practice for Surveillance Cameras and Personal Information, SCC The Surveillance Camera Code of Practice and the council's Data Protection Policy.

This policy covers the use of camera related surveillance equipment including

- Automatic Number Plate Recognition (ANPR)
- body worn video (BWV);

[2] GDPR comes into force 25th May 2018 superseding the DPA.

- unmanned aerial systems (UAS) aka Drones; and
- other systems that capture information of identifiable individuals or information relating to individuals.

Covert surveillance activity is not covered in this policy because this activity is governed by the Regulation of Investigatory Powers Act 2000. This type of recording is covert and directed at an individual or individuals. See the Council's' Surveillance Policy and Procedures.

3 Legislation

CCTV systems are subject to legislation under:

- Data Protection Act 1998 (DPA).
- Human Rights Act 1998 (HRA).
- Freedom of Information Act 2000 (FOIA).
- Regulation of Investigatory Powers Act 2000 (RIPA).
- General Data Protection Regulation (comes in force 25th May 2018)
- Protection of Freedoms Act 2012
- Criminal Procedures and Investigations Act 1996

4 Deciding when surveillance camera systems should be used

Using surveillance systems can be privacy intrusive. They are capable of placing large numbers of law-abiding people under surveillance and recording their movements as they go about their day-to-day activities.

Careful consideration should be given to whether or not to use a surveillance system. Taking into account the nature of the problem seeking to address; whether a surveillance system would be a justified and an effective solution, whether better solutions exist, what effect its use may have on individuals, and whether in the light of this, its use is a proportionate response to the problem.

Under the GDPR, there is a new legal obligation (Article 25) to implement Privacy by Design. This is an an approach that promotes privacy and data protection compliance from the start.

Under GDPR Data protection impact assessments (PIAs) (Ref GDR Article 35, 36) are mandatory for large scale CCTV monitoring surveillance. These will be conducted in consultation with the Council's Data Protection Office and ICO.

The ICO's have produced a (DPA) Conducting privacy impact assessments (July 2017) code of practice for good practice advice. The Surveillance Camera

Commissioner have produced PIAs specific to surveillance cameras Privacy impact assessments for surveillance cameras (Aug 2017)

The Council will use these guides to undertake PIAs and regularly evaluate whether it is necessary and proportionate to continue using CCTV..

5 Governance

For each CCTV deployment the lead Council Officer must :

- Produce and maintain a CCTV operational policy complying with the ICO Data Protection Code of Practice for Surveillance Cameras and Personal Information, SCC The Surveillance Camera Code of Practice and the Council's Data Protection Policy, including :

    - Data Controller/s details
    - Clear roles and responsibilities
    - Lawfulness condition
    - CCTV Objectives
    - Contracts in place with Data Processors (ref GDPR Article 30)
    - Contract monitoring arrangements
    - Compliance with CCTV standards
    - Administration
    - Security and Safeguard arrangements
    - Data quality
    - Record keeping procedures
    - Storing and viewing surveillance information
    - Disclosure
    - Dealing with subject access request
    - Retention and disposal
    - Staff Training
    - Siting surveillance cameras
    - Privacy notices
    - Using the equipment
    - Review and audit mechanism
    - Reporting arrangements

- Keep a record of PIAs and privacy by design documentation

- Keep a Register of data protection processing activity (ref GDPR Article 30)

- Undertake an annual review of CCTV using the Surveillance Camera Commissioner self assessment guide and implement actions:

Self assessment tool: surveillance camera code of practice (Aug 2016)
Self assessment tool: automatic number plate recognition (Aug 2016)
Self assessment tool: body worn video (Aug 2016)

6 References

Information Commissioner Office

https://ico.org.uk/

Data Protection Code of Practice for Surveillance Cameras and Personal Information (June 2017)

Surveillance Camera Commissioner

https://www.gov.uk/government/organisations/surveillance-camera-commissioner

The Surveillance Camera Code of Practice (June 2013)
A guide to the 12 principles (Oct 2014)
Steps to complying with the 12 principles (Oct 2014)

Privacy impact assessments for surveillance cameras (Aug 2016)

Self assessment tool: surveillance camera code of practice (Aug 2016)
Self assessment tool: automatic number plate recognition (Aug 2016)
Self assessment tool: body worn video (Aug 2016)

Recommended standards for the CCTV industry (Nov 2016)

7 Glossary

‘Data Controller’ [Data Protection Act 1998, General Data Protection Regulations) means who shall control, manage and determine the Objectives, and the manner in which any Data is to be processed. this can be a single or joint organisations;

Data Processor [Data Protection Act 1998, General Data Protection Regulations) A supplier contracted / authorised by the Data Controller to process the data.

“Data” includes personal Data, and all other processed information which is in the possession of the Data Controller which relates to property; or an individual or group of individuals who can be identified; which is processed by means of CCTV equipment operating automatically to further the Objectives

“Data Subject” an individual making a Data Subject Access Request

‘Objectives’ means the assessed purpose or reasons for installing the CCTV system; the assessed and required protections

Appendix A Data Protection Principles

The Data Protection Act 1998

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-

(a) at least one of the conditions in Schedule 2 is met, and
(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

General Data Protection Regulations

1 processed lawfully (Article 6, 9), fairly and in a transparent manner in relation to individuals;

2 collected for specified, explicit and legitimate purposes and not further processed

in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4 accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

6 processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7 The Data controller shall be responsible for and be able to demonstrate, compliance with the six principles.

Appendix B - The guiding principles of the Surveillance Camera Code of Practice

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 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.

Further guidance :

A guide to the 12 principles (Oct 2014)
Steps to complying with the 12 principles (Oct 2014)