ADUR & WORTHING
COUNCILS

Joint Governance Committee
28 May 2020
Agenda Item 12

Ward(s) Affected: All

Update of the CCTV Policy

Report by the Director for Digital & Resources

Executive Summary

1. Purpose

- To update the Adur & Worthing Councils' CCTV Policy and make it compliant with the current legislation and guidance.
- To ensure compliance with data protection legislation and to ensure that good operational arrangements are in place.

2. Recommendations

2.1 That the Joint Governance Committee, on behalf of the Councils, reviews and approves the CCTV (Closed Circuit Television) Policy v2.0

3. Context

- The CCTV (Closed Circuit Television) Policy v1.0 was reviewed and approved by the Joint Governance Committee on 28/11/17.
- Since then the Data Protection Act 1998 was repealed and replaced by the Data Protection Act 2018 and the General Data Protection Regulation.
- The Surveillance Camera Commissioner's and Information Commissioner's guidance was also updated.

4. **Issues for consideration**

    - No new obligations are introduced by the updated Policy, apart from the requirement to conduct a Data Protection Impact Assessment using the Surveillance Camera Commissioner's standard templates.

5. **Engagement and Communication**

    - No internal or external engagement.

6. **Financial Implications**

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

7. **Legal Implications**

    - Policy reviewed and agreed by Legal Officer.
    - The processing of personal data must comply with the Data Protection Act 2018 and the General Data Protection Regulation.
    - The Joint ADC and WBC Surveillance Policy and Procedure is a separate policy covering covert surveillance and governed by the Regulation of Investigatory Powers Act 2000. It is maintained by the Councils' Monitoring Officer in Legal Services.

Background Papers

- Draft CCTV (Closed Circuit Television) Policy v2.0 (attached below)
- The CCTV (Closed Circuit Television) Policy v1.0
- Joint Governance Committee 28 November 2017 - Item 9 - CCTV Policy

Officer Contact Details:-
Marina Koltsova
Senior Information Governance Officer
01903221251
marina.koltsova@adur-worthing.gov.uk

Sustainability & Risk Assessment

1. Economic

- Matter considered and no issues identified.

2. Social

2.1 Social Value

- It ensures that data protection and individuals' information rights are taken into consideration when CCTV is used by the Councils.

2.2 Equality Issues

- Matter considered and no issues identified.

2.3 Community Safety Issues (Section 17)

- It enables usage of CCTV for community safety purposes that is compliant with the data protection legislation.

2.4 Human Rights Issues

- This Policy is intended to ensure that human rights, the right to privacy in particular, are considered prior to and during the operation of CCTV. The appropriate use of Data Protection Impact Assessments and CCTV self assessments would demonstrate the Councils' compliance with human rights.

3. Environmental

- Matter considered and no issues identified.

4. Governance

- Matter considered and no issues identified.

Closed Circuit Television (CCTV) Policy

Date	Version number	Changes
28/11/17	1.0	Approved by Joint Governance Committee
	2.0 DRAFT	

1. Introduction

Images recorded by surveillance systems identifying a living individual are personal data which must be processed in accordance with data protection laws. 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 2018 (DPA) and General Data Protection Regulation (GDPR).

2. Purpose and scope

This policy details the good practice standards recognised by the Information Commissioner's Office and the 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 encourage compliance with the Surveillance Camera Code of Practice. The Councils must have regard to this Code of Practice when implementing surveillance camera systems covered by the Code. See **Appendix A** for the 12 guiding principles contained in the Code of Practice.

This policy document must be read in conjunction with the SCC The Surveillance Camera Code of Practice and the Council's Data Protection Policy.

By following these provisions the Council will ensure that arrangements are both fair and lawful.

This policy covers the use of camera related surveillance equipment including

- Automatic Number Plate Recognition (ANPR)
- body worn video (BWV);
- 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 (available on the Intranet).

This policy covers all employees, officers, consultants and volunteers. This policy may be amended at any time and does not form part of the terms and conditions of any employment or other contract.

3. 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 legal obligation (Article 25) to implement data protection by design and by default. This means integrating data protection concerns into every aspect of the Councils' processing activities.

Under the GDPR Data Protection Impact Assessments (DPIAs) (Ref GDPR Article 35, 36) are mandatory for large scale CCTV monitoring surveillance. These will be conducted in consultation with the Council's Data Protection Officer and, if necessary, the ICO.

The Council will use the SCC's Data Protection impact assessments for surveillance cameras (Aug 2017), the Surveillance Camera Code of Practice and the ICO's Data Protection impact assessments guidance for good practice advice when evaluating the use of CCTV.

4. Governance

For each CCTV deployment the lead Council Officer for the project must :

1. Contact the Councils' Data Protection Officer with completed copies of the three documents contained within **Appendix B**.

2. Ensure that the Register of Processing Activity (ROPA - ref GDPR Article 30) is updated where necessary to reflect the new processing.

3. Undertake and maintain records of an annual review of CCTV using the Surveillance Camera Commissioner's self assessment tool.

5. Document Review

This policy will be reviewed annually by the Data Protection Officer.

6. References & Guidance

- The Surveillance Camera Code of Practice
- A guide to the 12 principles
- Steps to complying with the 12 principles
- Data Protection impact assessment: carrying out a data protection impact assessment on surveillance camera systems)
- Self assessment tool: surveillance camera code of practice
- Recommended standards for the surveillance camera industry

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

System operators should adopt the following 12 guiding principles:

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.

Appendix B - SCC data protection impact assessment templates and guidance

SURVEILLANCE CAMERA COMMISSIONER

Data protection impact assessments

template for carrying out a data protection impact assessment on surveillance camera systems

Project name:

Data controller(s):

This DPIA template should be completed with reference to the guidance provided by the Surveillance Camera Commissioner and the ICO. It will help you to identify whether the use of surveillance cameras is appropriate for the problem you wish to address, assess the risks attached to your project and form a record of your decision making.

1. Identify why your deployment of surveillance cameras requires a DPIA[1]:

☐ Systematic & extensive profiling	☐ Large scale use of sensitive data
☐ Public monitoring	☐ Innovative technology
☐ Denial of service	☐ Biometrics
☐ Data matching	☐ Invisible processing
☐ Tracking	☐ Targeting children / vulnerable adults
☐ Risk of harm	☐ Special category / criminal offence data
☐ Automated decision-making	☐ Other (please specify)

2. What are the timescales and status of your surveillance camera deployment? Is this a proposal for a new deployment, or the expansion of an existing surveillance camera system? Which data protection regime will you be processing under (i.e. DPA 2018 or the GDPR)?

Describe the processing

3. Where do you need to use a surveillance camera system and what are you trying to achieve? Set out the **context** and **purposes** of the proposed surveillance cameras or the reasons for expanding an existing system. Provide evidence, where possible, including for example: crime statistics over an appropriate time period; housing and community issues, etc.

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/

4. Whose personal data will you be processing, and over what area? Set out the **nature** and **scope** of the personal data you will be processing. Who are the data subjects, and what kind of information will you be collecting about them? Do they include children or vulnerable groups, and what is the scale and duration of the processing?

5. Who will be making decisions about the uses of the system and which other parties are likely to be involved? Will you be the sole user of the data being processed or will you be sharing it with other organisations or agencies? Record any other parties you would disclose the data to, for what purposes, and any relevant data sharing agreements. Note that if you are processing for more than one purpose you may need to conduct separate DPIAs.

6. How is information collected? (tick multiple options if necessary)

- ☐ Fixed CCTV (networked)
- ☐ Body Worn Video
- ☐ ANPR
- ☐ Unmanned aerial systems (drones)
- ☐ Stand-alone cameras
- ☐ Redeployable CCTV
- ☐ Other (please specify)

7. Set out the information flow, from initial capture to eventual destruction. You may want to insert or attach a diagram. Indicate whether it will include audio data; the form of transmission; the presence of live monitoring or use of watchlists; whether data will be recorded; whether any integrated surveillance technologies such as automatic facial recognition are used; if there is auto deletion after the retention period. You may have additional points to add that affect the assessment.

8. Does the system's technology enable recording?

☐ Yes ☐ No

If recording is enabled, state where it is undertaken (no need to stipulate address, just Local Authority CCTV Control room or on-site will suffice for stand-alone camera or BWV), and whether it also enables audio recording.

9. If data is being disclosed, how will this be done?

☐ Only by on-site visiting

☐ Copies of footage released (detail method below, e.g. encrypted digital media, via courier, etc)

☐ Off-site from remote server

☐ Other (please specify)

10. How is the information used? (tick multiple options if necessary)

☐ Monitored in real time to detect and respond to unlawful activities

☐ Monitored in real time to track suspicious persons/activity

☐ Compared with reference data of persons of interest through processing of biometric data, such as facial recognition.

☐ Compared with reference data for vehicles of interest through Automatic Number Plate Recognition software

☐ Linked to sensor technology

☐ Used to search for vulnerable persons

☐ Used to search for wanted persons

☐ Recorded data disclosed to authorised agencies to support post incident investigation, including law enforcement agencies

☐ Recorded data disclosed to authorised agencies to provide intelligence

☐ Other (please specify)

Consultation

11. Record the stakeholders and data subjects you have consulted about the deployment, together with the outcomes of your engagement.

Stakeholder consulted	Consultation method	Views raised	Measures taken

Consider necessity and proportionality

12. What is your lawful basis for using the surveillance camera system? Explain the rationale for your chosen lawful basis under the relevant data protection legislation. Consider whether you will be processing special categories of data.

13. How will you inform people that they are under surveillance and ensure that they are provided with relevant information? State what privacy notices will be made available and your approach to making more detailed information available. Consider whether data subjects would reasonably expect to be under surveillance in this context.

14. How will you ensure that the surveillance is limited to its lawful purposes and the minimum data that is necessary for those purposes? Explain the adequacy and relevance of the data you will be processing and how it is limited to the purposes for which the surveillance camera system will be deployed. How will you know if it is delivering the benefits it has been deployed for?

15. How long is data stored? (please state and explain the retention period)

16. Retention Procedure

☐ Data automatically deleted after retention period

☐ System operator required to initiate deletion

☐ Under certain circumstances authorised persons may override the retention period, e.g. retained for prosecution agency (please explain your procedure)

17. How will you ensure the security and integrity of the data? How is the data processed in a manner that ensures appropriate security, protection against unauthorised or unlawful processing and against accidental loss, destruction or damage? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

18. How will you respond to any subject access requests, the exercise of any other rights of data subjects, complaints or requests for information? Explain how you will provide for relevant data subject rights conferred under the legislation. You must have procedures in place to respond to requests for camera footage in which a subject appears, and to respond to any other request to meet data protection rights and obligations.

19. What other less intrusive solutions have been considered? You need to consider other options prior to any decision to use surveillance camera systems. For example, could better lighting or improved physical security measures adequately mitigate the risk? Does the camera operation need to be continuous? Where you have considered alternative approaches, provide your reasons for not relying on them and opting to use surveillance cameras as specified.

20. Is there a written policy specifying the following? (tick multiple boxes if applicable)

☐ The agencies that are granted access

☐ How information is disclosed

☐ How information is handled

Are these procedures made public? ☐ Yes ☐ No

Are there auditing mechanisms? ☐ Yes ☐ No

If so, please specify what is audited and how often (e.g. disclosure, production, accessed, handled, received, stored information)

Identify the risks

Identify and evaluate the inherent risks to the rights and freedoms of individuals relating to this surveillance camera system. Consider, for example, how long will recordings be retained? Will they be shared? What are the expectations of those under surveillance and impact on their behaviour, level of intrusion into their lives, effects on privacy if safeguards are not effective? Could it interfere with other human rights and freedoms such as those of conscience and religion, expression or association. Is there a risk of function creep? Assess both the likelihood and the severity of any impact on individuals.

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**

	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Address the risks

Explain how the effects of privacy enhancing techniques and other features mitigate the risks you have identified. For example, have you considered earlier deletion of data or data minimisation processes, has consideration been given to the use of technical measures to limit the acquisition of images, such as privacy masking on cameras that overlook residential properties? What security features, safeguards and training will be in place to reduce any risks to data subjects. Make an assessment of residual levels of risk.

Note that APPENDIX ONE allows you to record mitigations and safeguards particular to specific camera locations and functionality.

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk			
Options to reduce or eliminate risk	**Effect on risk**	**Residual risk**	**Measure approved?**
	Eliminated reduced accepted	Low medium high	Yes/no

Authorisation

If you have not been able to mitigate the risk then you will need to submit the DPIA to the ICO for prior consultation. Further information is on the ICO website.

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion.

Residual risks approved by:		If you identify a high risk that you cannot mitigate adequately, you must consult the ICO before starting to capture and process images.
DPO advice provided by:		DPO should advise on compliance and whether processing can proceed.
Summary of DPO advice		
DPO advice accepted or overruled by: (specify role/title)		If overruled, you must explain your reasons.
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons.
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA.

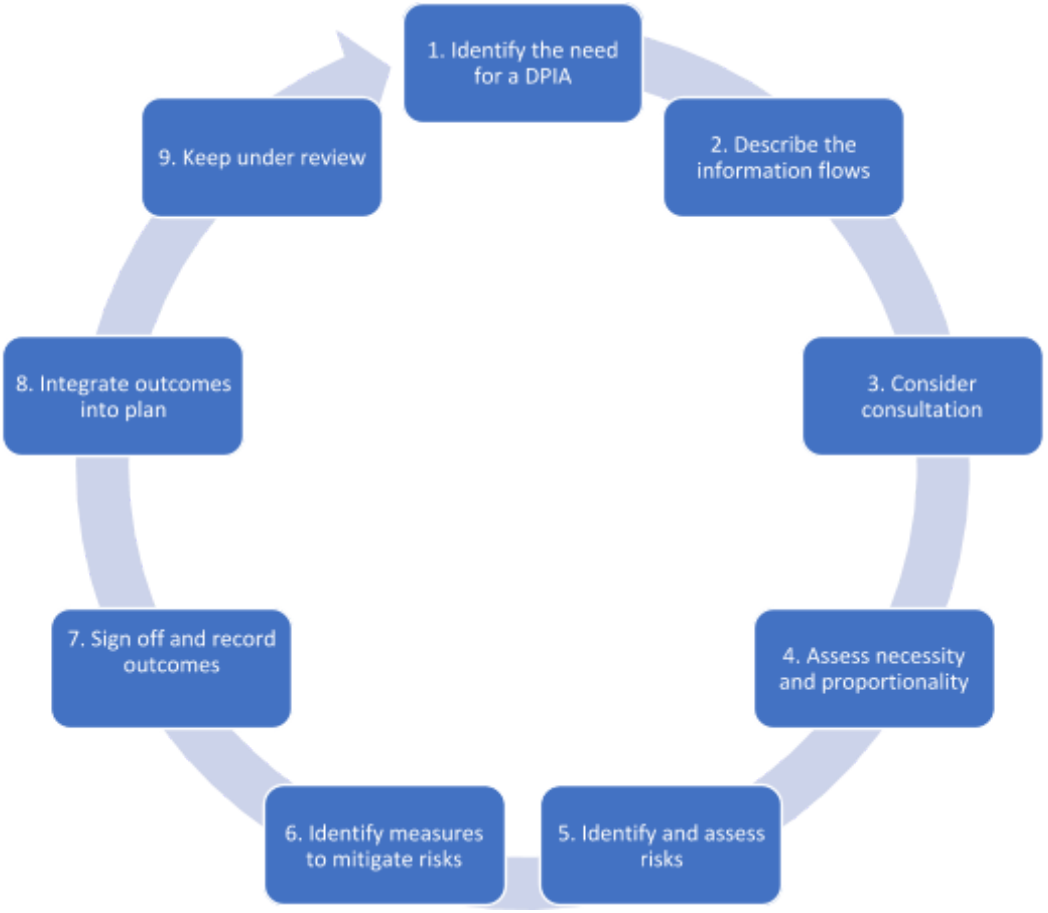
APPENDIX ONE

This template will help you to record the location and scope of your surveillance camera system and the steps you've taken to mitigate risks particular to each location.

Location: Each system operator/owner should list and categorise the different areas covered by surveillance on their system. Examples are provided below.

Location type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
Town centre	All	250	24hrs	24hrs (only maximum 3 operators) – likely average patrol high hourly	The privacy level expectation in a town centre is very low; our town centres are well signed with appropriate signage for CCTV its use and purpose with contact details.
Public car park	1, 5, 6	100			
Parks					HD camera only include due to proximity to town HD cam
Play areas					
Housing blocks internal	1, 2	200	24hrs (calendar month)	Limited due to the fact that most are static cameras	High level asb historical problems (please see statistical assessment in annual review)
Housing estate (street)					
Residential street					Cameras are installed here to respond to high crime trends, deal with the fear of crime

APPENDIX TWO: STEPS IN CARRYING OUT A DPIA



APPENDIX THREE: DATA PROTECTION RISK ASSESSMENT MATRIX

Use this risk matrix to determine your score. This will highlight the risk factors associated with each site or functionality.

Matrix Example:

	Camera Types (low number low impact – High number, High Impact								
Location Types A (low impact) Z (high impact)									