SURVEILLANCE CAMERA COMMISSIONER

ico.
Information Commissioner's Office

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

Project name: Cullompton Town CCTV

Data controller(s): Cullompton Town Council

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)

For the detection and deterrence of crime.

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)?

Existing CCTV installation.

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.

For the detection and deterrence of crime. The system is used by the Police to provide primary and secondary evidence where a crime has been committed. For instance, there have been a number of road traffic collisions, including one fatality, in the CCTV surveillance area and the CCTV system provided valuable evidence in securing convictions.

In addition, it has been used to identify persons of interest in cases of violence and anti-social behaviour as a result of the late-night economy.

[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?

All cameras are located in public spaces, and do not target specific individuals or group demographics. Data collected is not of a person-specific nature, and, in specific cases such as Subject Access Requests, all irrelevant data will be redacted.

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.

Decisions will be made strictly in accordance with the Home Office Model CCTV Code of Practice as adopted by Cullompton Town Council in March 2023,

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.

Information is captured to a recording device and retained for approximately 6 weeks, after which it is automatically overwritten. Should the Police request footage, it will be reviewed before seizure to ensure that it's retention and distribution within the evidence gathering and prosecution systems are strictly necessary. The system is entirely passive, is not monitored by operatives, and no facial recognition or ANPR is deployed.

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.

Video images are recorded in a password protected device, located in a secure room in a locked building. Access is limited to two members of staff.

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)

Video footage will be viewed remotely (using SmartPSS software) and, it if is required to be seized for evidential purposes, it will be supplied to authorised and identified Police Officers and Police Community Support Officers either by securing the footage to a USB memory stick, or by sending footage over the GoodSam secure online file transfer system used by the Police.

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
Police Service	Email	I'm aware we have sent various requests for footage since your last review. We are most grateful for your help with this, and It is clear the system ads a lot of value in various ways, such as: • Reassurance for the general public. • We have used footage to secure convictions • We have used the footage to identify offenders. As-such I can confirm that the local police fully support the retention of the system for the purposes of the deterrence, detection, and investigation of crime.	None.

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.

For the detection and deterrence of crime.

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.

There is compliant signage informing all who enter the CCTV monitored area that they are doing so. All cameras are visible, and none are considered to be covert.

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?

The recording device is password protected, in a secure room, in a locked building. Only two Council employees have access to the system, and will only do so in accordance with the Home Office Model CCTV Code of Practice and at the request of authorised Agencies.

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

Approximately 6 weeks, after which data is automatically overwritten.

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)

Shoud data require retention, that retention will be to a USB memory stick or GoodSam data transfer to authorised and identified individuals representing authorised Agencies.

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?

The recording device is password protected and located in a secure room in a locked building. Only two Town Council employees are authorised to access the system, and will only do so when authorised to do so using guidance from the Home Office Model CCTV Code of Practice.

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.

Subject Access Requests (SAR) will be complied with provided that a very narrow window of time is provided by the SAR applicant and, before any data is handed to the SAR applicant, all other data not relevant to the SAR request will be redacted.

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.

For the purposes of the CCTV system, that is the detection and deterrence of crime, it is considered to be the only option, particularly for the retrospective detection and investigation of crime.

Date and version control: 19 May 2020 v.4

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)

Date and version control: 19 May 2020 v.4

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**
Retention of Data. Data is retained for approximately 6 weeks, after which it is automatically overwritten.	Remote, possible or probable Remote	Minimal, significant or severe Minimal	Low, medium or high Low
Access to Data. Data is only accessed by one of two authorised employees of Cullompton Town Council at the request of authorised and identified representatives of authorised Agencies.	Remote	Minimal	Low
Sharing of Data. Data is only shared with authorised and identified representatives of authorised Agencies and only when provided with a relatively narrow window of time. Data will be reviewed before seizure to ensure that it is not being used for a "fishing trip".	Remote	Minimal	Low
Expectations. Anecdotally, the public support the presence of the system and, whilst crime and anti-social behaviour does occur, it is considered that the presence of the CCTV system does deter most instances of it.	Remote	Minimal	Low

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**
Level of Intrusion. Level of intrusion in the personal lives of individuals is considered minimal as, whilst recorded footage is stored, it is only accessed and/or retained in specific circumstances in accordance with the adopted Home Office Model CCTV Code of Practice. Private spaces, such as residential dwellings, are masked from recordings.	Remote, possible or probable Remote	Minimal, significant or severe Minimal	Low, medium or high Low
Infringement of Rights. It is not considered that the presence of the CCTV system infringes on other rights and freedoms, such as conscience and religious freedoms or other associations.	Remote	Minimal	Low
Function Creep. The two authorised operators of the CCTV system remain vigilant regarding the nature of the requests made, and the legislation under which the request is made. Should function creep become apparent, operators will refuse access to the data.	Possible	Significant	Medium

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?**
Function Creep. Access to the recorded footage is limited to two members of staff who will consult prior to accessing recorded imagery and remain vigilant of function creep of the CCTV system.	Eliminated reduced accepted Accepted	Low medium high Medium	Yes/no Yes

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: Town Clerk	Dan Ledger	Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by: Town Clerk	Dan Ledger	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: Not applicable	Existing system.	DPO should advise on compliance and whether processing can proceed.
Summary of DPO advice Not applicable		
DPO advice accepted or overruled by: (specify role/title)	Not applicable	If overruled, you must explain your reasons.
Comments: Existing system.		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons.
Comments: Existing System.		

Date and version control: 19 May 2020 v.4

This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA.

Date and version control: 19 May 2020 v.4

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 Hall	Fixed	1	Yes	Interior of Town Hall publc lobby	Monitoring access to the Town Hall public spaces in the event that items are removed.
Town Centre	Fixed	12	Yes	Town Centre Pubic Spaces	Monitoring of Town Centre public spaces for the detection and deterrence of crime and anti-social behaviour.
Cemetery	Fixed	3	Yes	Cemetery Public Spaces	Monitoring the car park and storage areas of the Cemetery for the detection and deterrence of crime and anti-social behaviour.

Date and version control: 19 May 2020 v.4

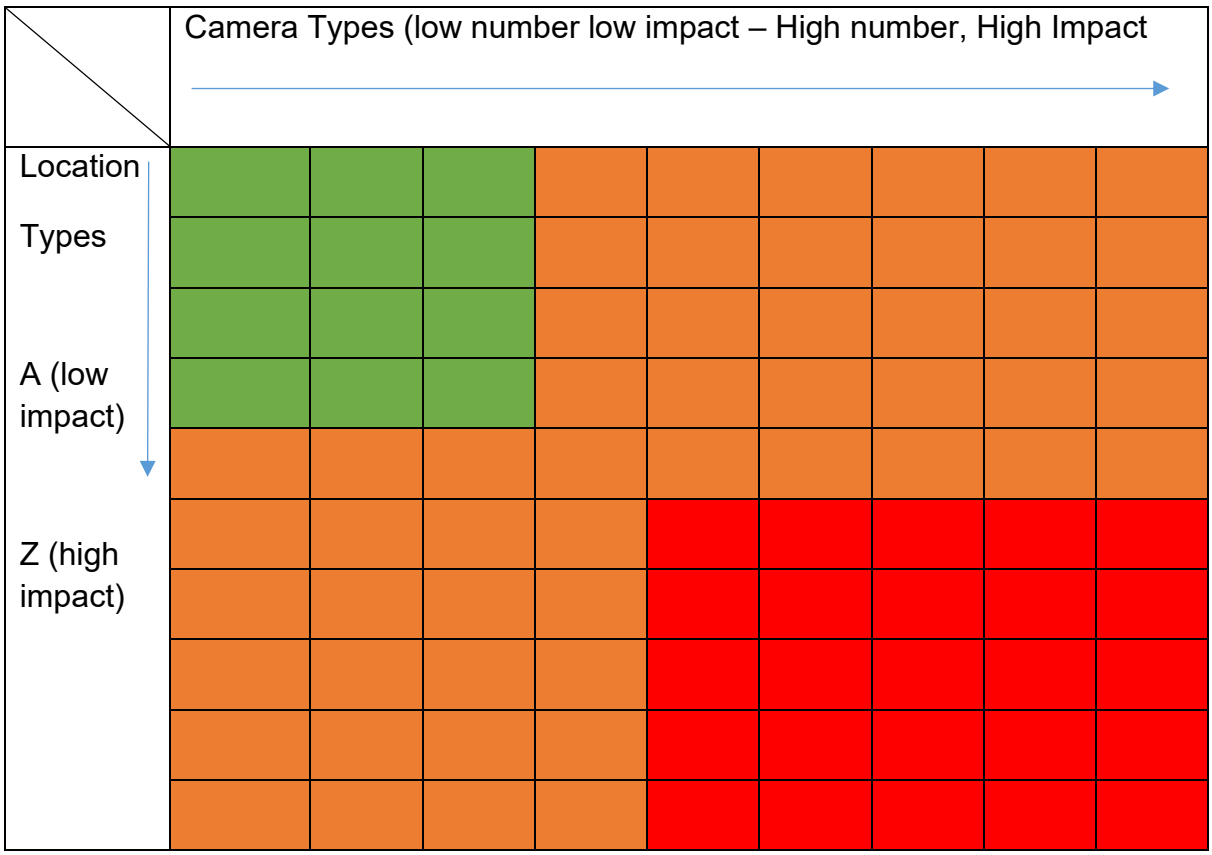
APPENDIX TWO: STEPS IN CARRYING OUT A DPIA

Date and version control: 19 May 2020 v.4

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:



Date and version control: 19 May 2020 v.4

NOTES

Date and version control: 19 May 2020 v.4

Date and version control: 19 May 2020 v.4