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: Runnymede Borough Council - Public Space CCTV Scheme October 2021

Data controller(s): Runnymede Borough 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)

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)?

Annual review of existing Public Space CCTV system.

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.

The role of the Safer Runnymede CCTV scheme is to support and assist in the detection and prevention of crime and anti-social behaviour by acting either as an overt deterrent or where crime is committed, in providing video evidence to support prosecutions.

[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?

For the purposes of the detection of crime or any ASB, all recorded images should be capable of identifying individuals who may be suspects, or victims or witnesses of a criminal offence.

Identifying factors required for evidential purposes would include location, stature, IC code, clothing and/or distinctive features or items being carried together with any vehicle make, model, type, colour together with any visible vehicle registration number.

For public safety monitoring purposes of CCTV, the majority of recorded images would be of sufficient quality as to be admissible in relation to personal data where the CCTV camera was being used by an Operator to monitor an incident in real time or prior to or immediately after a specific event.

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.

Runnymede Borough Council has a dedicated Data Protection Officer (DPO) and a Corpoate Head of Service Director - Head of Law and Governance nominated and responsible for the role of Senior Responsible Officer. The SCC has been notified of those responsible individuals.

Other data processors include:

1) The signatories to the Surrey Police Data Sharing Agreement
2) Those authorised to carry out investigations (Trading Standards, Environmental Health. Corporate Fraud) etc.
3) Statutory authorities responsible for prosecutions of Data subjects

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.

CCTV video data (audio is not captured) is transmitted electronically by various secure means from the CCTV camera to a purpose-built CCTV Centre which is manned 24x7/365. This data is recorded and stored in video format within a secure server room.

Access is restricted to authorised staff only.

Received video images are delivered from the recording devices (cameras) to the staff monitoring them within the secure CCTV Centre. The retention period of captured video data is 31 days after which time the data is automatically deleted from the system without the need for manual intervention unless the data is requested by an authorised person in pursuance of a criminal or civil investigation. If this is the case, the data will be copied form the system and an evidence pack created.

Detailed procedures and policies exist within the Council to ensure that the recorded data is handled, used and deleted in the most appropriate and lawful manner. All CCTV staff have received relevant training in legislation, procedures and the effective use of the system. These staff are qualified to BTeC standards, and refreshers are regularly undertaken.

Video boimetrics technologies,such as facial recogniton, are not used.

Staff are subject to vetting by Sussex/Surrey Police to NPPV2 level.

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.

System wide video recording is in place at Safer Runnymede - CCTV control room.

There is no 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
Local residents	Letter	1 x Privacy concern	Electronic data privacy zone applied to camera view
Surrey Poilce (Monthly)	Joint Action Group - Community Safety Partnership	Various	Ongoing operational collaboration within the criteria set out withint the data sharing agreement and CCTV code of practice.

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.

GDPR Article 6(1)(e): Processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the data controller.

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.

Runnymede Borough Council (RBC) use their own specific and ICO approved CCTV signage which is displayed at each CCTV camera site.

Processes for Subject Access Requests (SAR) and/or any CCTV related complaints are detailed on the Council's website and are available from the CCTV Centre manager or from the RBC Corporate Complaints team.

RBC website shows the locations of all our CCTV cameras, along with information on how to request data

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?

Runnymede CCTV video data is used effectively for criminal and civil investigations whilst at all times observing the respect for the right to privacy.

The data will only be used for those purposes stated within this document.

All of our video cameras/system are installed, maintained and operated professionally, providing high quality primary and secondary video evidence for investigators to use.

We will only share CCTV evidence with bona-fide individuals/organisations and only when those who have a legitimate need for data have demonstrated that they will process data in a proportionate and appropriate manner.

We will measure statistical benefit annually for year on year analysis. That said, it remains difficult to quantify the deterrent value of the system.

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

31 Days and then automaticallt over-written ubnless otherwise requested for download and sharing by those agnecies referenced in Q5 (above)

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?

The Council's CCTV system is closed. Access is obtained using unique security criteria.

All data sharing is considered within the Code of Practice with no unauthorised data sharing.

Policy requires any Council officer or official seeking to use CCTV to first consult with the CCTV SPOC (CCTV Centre Manager). This policy delivers consistency of approach and good governance.

The policy is available on the public website.

There are no 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.

The process for Subject Access Requests is detailed on the Council's website.

RBC website shows the locations of all our CCTV cameras (excepting redeployable CCTV), along with information on how to request data.

As the redeployable CCTV assets are often moved, any data requests regards Redeployable CCTV will be dealt with by the CCTV manager.

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)

Access to the system is via unique log in.
System access tracking can be audited where required.
Evidential downloads/uploads are strictly controlled and only authorised staff can carry out those functions.
All evidential downloads/uploads have a unique identifier.

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**
A public space CCTV system is necessarily placed to capture video data that in some circumstances, might intrude upon the individual rights and freedoms of those whom it regularly views. Our CCTV code of parctice, our staff training, our legislative awareness, our leadership and our general good practice mitigate against those risks to the public. Where surveillance WILL infringe upon those rights and freedoms, we insist that the appropriate legislation e.g. RIPA be applied PRIOR to any operational mobilisation.	Remote, possible or probable Remote	Minimal, significant or severe Minimal	Low, medium or high 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**
Risk to privacy	Remote, possible or probable Remote	Minimal, significant or severe Significant	Low, medium or high Low

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?**
Digital Privacy Zones (DPZ) can be applied to CCTV camera views to eliminate those concerns raised by Public/Business users.	Eliminated reduced accepted Eliminated	Low medium high Low	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:		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:		

Date and version control: 19 May 2020 v.4

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

Date and version control: 19 May 2020 v.4

APPENDIX ONE

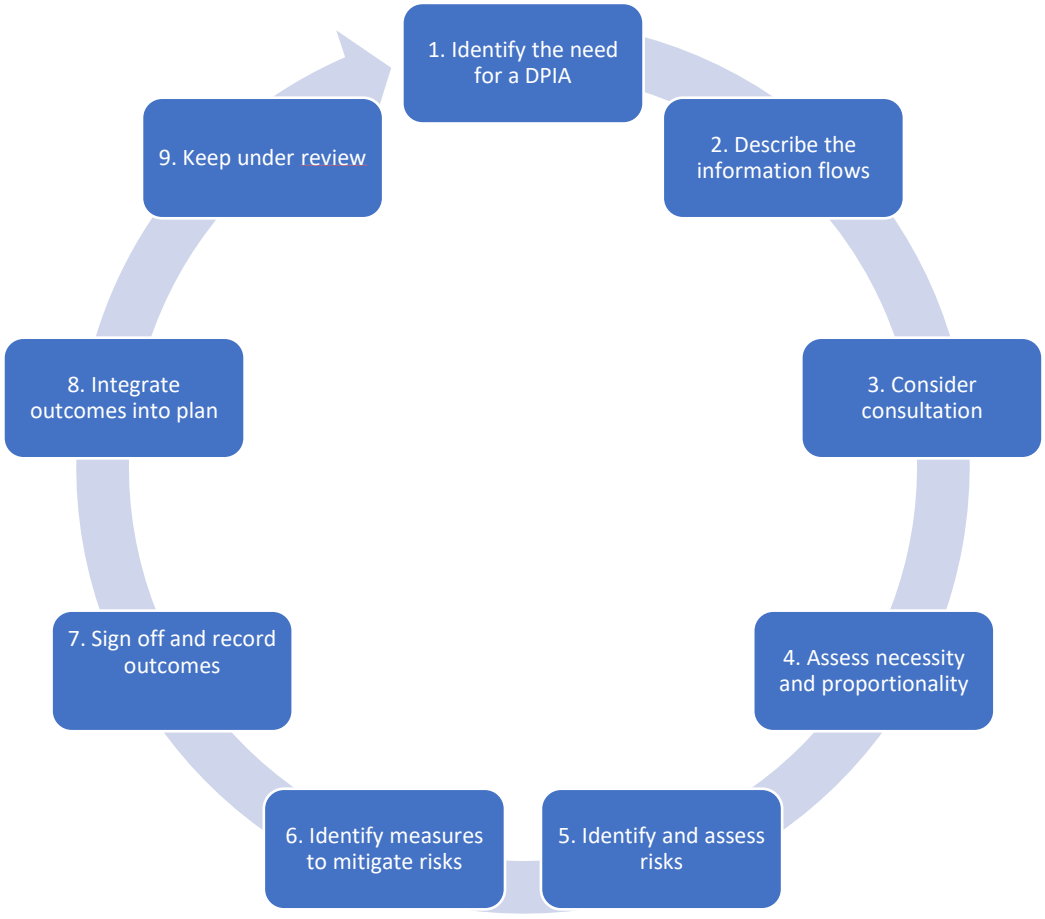
This template will help you to record the location and scope of your surveillance camera system and the steps you've taken to mitigate risks particular to each location.

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 centre	Pan tilt Zoom (PTZ)/Fixed panoramic/Fixed	152	24hrs	24hrs	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	PTZ/360	47	24 Hrs	As above	Cameras are installed here to deal with the fear of crime and support residents
Independent retirement Housing	PTZ/Fixed	59	24 HRS	As above	Cameras are installed here to deal with the fear of crime and support residents
Redeployable CCTV	PTZ	9	24 HRS	As above	Cameras are installed here to respond to high crime trends, deal with the fear of crime and support residents
Housing blocks internal	FIXED 360	10	24 HRS	As above	Cameras are installed here to deal with the fear of crime and support residents

Date and version control: 19 May 2020 v.4

APPENDIX TWO: STEPS IN CARRYING OUT A DPIA

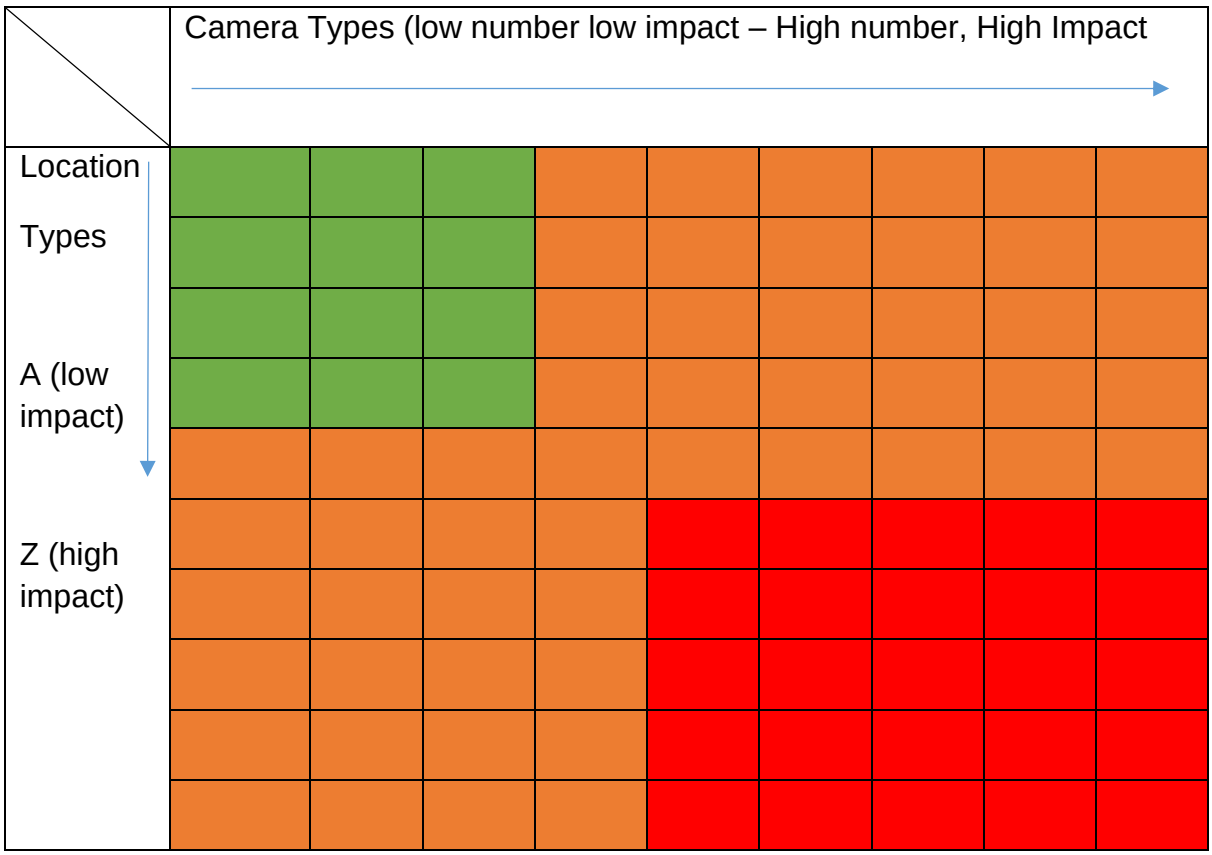


Date and version control: 19 May 2020 v.4

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

Assuming a maximum materix risk score of 90 where locations = max 10 x number of camera types = max 9.

Runnymede CCTV has locations x 5 and type x 3. Score = 15/90

Date and version control: 19 May 2020 v.4

Date and version control: 19 May 2020 v.4