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: Cayton Parish Council Public Space Surveillance CCTV System

Data controller(s): Cayton Parish 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)

Pubclic space and entry/exit monitoring of Jubilee Hall for crime prevention and detection of crime and public safety.

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)?

The system is a new surveillance system and will be deployed in a phased manner following installation, testing and commissioning. Once operational, it will be continuously monitored, routinely maintained and periodically reviewed and certified in accordance with the Surveillance Camera Code of Practice (SCC) and all relevant governing guidance and standards.

The lawful basis for processing personal data is Article 6(1)(e) UK GDPR – processing is necessary for the performance of a task carried out in the public interest and/or in the exercise of official authority vested in the controller. The deployment of the system supports the Council's statutory functions, including community safety, crime prevention and detection, and the protection of public spaces.

The system will operate on an ongoing basis, subject to regular governance review to ensure that its use remains necessary, proportionate and effective for the stated purposes. Any expansion, relocation or material change to the system will be subject to further assessment, including a review of this DPIA where required.

[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/

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 proposed surveillance cameras will be installed at key access points at Jubilee Hall, specifically at the main entrance and the fire exit. These locations have been identified as higher risk areas due to increased footfall and reduced natural surveillance at certain times.

The purpose of the system is to prevent and detect crime, improve public safety, and reduce anti social behaviour in and around Jubilee Hall. The cameras will provide a visible deterrent and assist in the identification and investigation of incidents such as damage to property, unauthorised access, and disorderly behaviour, particularly outside staffed hours.

Camera coverage will be limited to the immediate vicinity of these access points and will be configured to avoid unnecessary intrusion into private areas. Recorded footage will be accessed only by authorised personnel and used solely for legitimate purposes in accordance with the Surveillance Camera Code of Practice and data protection legislation.

The use of surveillance cameras at Jubilee Hall is considered necessary and proportionate to support a safe and secure environment for staff, visitors, and the wider community.

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?

The surveillance camera system will process the personal data of members of the public, including staff, visitors and contractors, who pass through the monitored areas at Jubilee Hall. This may include children and vulnerable individuals, as the premises are used by the wider community; however, no targeted monitoring of any group will take place.

Cameras will monitor limited and specific areas only, namely the main entrance and fire exit. Coverage will be restricted to these access points and will not capture private areas beyond what is necessary. The data processed will include visual images and audio recordings. The system does not use facial recognition, profiling, behavioural analysis or any other automated decision making or analytical software, and it does not discriminate in any way.

Processing is small scale and proportionate, with recordings retained for a limited period in accordance with the Council's retention policy, unless required for the investigation of an incident. Access to recordings will be restricted to authorised personnel only.

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.

The data owner and data controller is Cayton Parish Council. The council will share data with

1. Data subjects
2. Statutory prosecuting authorities
3. Clients and authorised investigators
4. Cayton Jubilee Hall Management Committee (Chairty Number 508873)

No other organisation will have access to the data other than general individuals exercising their rights in relation to subject access requests.
Date

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.

Video and audio data will be captured by fixed surveillance cameras located at the agreed sites. The system is hard wired, and footage is transmitted securely to the Council's CCTV system with no wireless public transmission.

Footage is recorded and is also available for live monitoring by authorised and trained personnel via a CCTV monitor or secure phone application. No watchlists, profiling, automatic alerts or integrated surveillance technologies (including facial recognition or automated analytics) are used.

Recorded footage is stored securely and retained for a standard retention period of 30 days, after which it is automatically deleted. Where footage is required for a specific lawful purpose—such as the investigation of a major incident, civil proceedings, or a valid Subject Access Request—it may be retained for longer in a secure evidence storage environment and deleted once no longer required.

Access to live or recorded footage is limited to authorised personnel who have received appropriate training in Council policies, procedures and system use. Any disclosure of footage is carried out in accordance with Council data sharing procedures, statutory powers and the principles of UK GDPR and the Data Protection Act 2018.

All processing, storage, sharing and deletion of data is managed in line with Council security standards and information governance policies.

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 and audio recording takes place on site.

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)

Police/statutory prosecuting authorities will access data on site. Subject Access requests, requests from Insurance Companies and solicitors will be dealt with by using encrypted media and courier or recorded delivery.

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)

Released to North Yorkshire Council departments invesrtigating ASB, Licensing and Fly Tipping.

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
Jubilee Hall	Email	Jubilee Hall requested that cameras be installed to address ongoing crime and to be a visual deterant, following ongoing items going missing and requests from hall users.	Added to Full Council Meeting agenda and sought quotes for cameras. Public were also invited to attend where they could ask questions about anything on the agenda.
North Yorkshire Councillor	In person	Supported the use of cameras for the prevention of incidents, visual deterant and to support the investigation of incidents	Added to Full Council Meeting agenda and sought quotes for cameras. Public were also invited to attend where they could ask questions about anything on the agenda.

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.

The lawful basis for processing is Article 6(1)(e) UK GDPR – processing is necessary for the performance of a task carried out in the public interest and in the exercise of official authority vested in the controller.

Cayton Parish Council, as a public authority, operates the surveillance camera system in support of its responsibilities relating to crime prevention, public safety, and community reassurance within the parish. These functions are supported by Section 17 of the Crime and Disorder Act 1998, which places a duty on local authorities to have due regard to the prevention of crime and disorder, and Section 163 of the Criminal Justice and Public Order Act 1994, which provides powers for local authorities to install and operate CCTV systems for the purposes of crime prevention and public welfare.
The use of CCTV is considered necessary and proportionate to achieve these aims and forms part of a wider, coordinated approach to reducing crime and anti social behaviour.

The system is not intended to process special category data. However, such data may be captured incidentally (for example, images or audio revealing health or other protected characteristics). Where this occurs, processing is justified as necessary for reasons of substantial public interest under Article 9(2)(g) UK GDPR, with appropriate safeguards in place and processing limited to what is strictly necessary.

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.

Cayton Parish Council will ensure transparency by clearly informing individuals that surveillance is in operation. Prominent CCTV signage is displayed at the monitored locations, advising that video and audio recording is taking place, the purpose of the system, and the identity of the data controller. Further information is provided through the Council's privacy notice, which is published on the Parish Council website and explains how personal data is processed, the lawful basis, retention periods, and individuals' rights, including how to submit Subject Access Requests.

The purchase and installation of the CCTV system were included on a Full Council meeting agenda, which is publicly available on the Council's website, ensuring transparency and public accountability. In addition, the Jubilee Hall Management Committee was asked to notify all regular hall users of the introduction of the CCTV system.

Engagement with the local community has also taken place, including a Parish Councillor speaking directly with the local school to raise awareness of the CCTV system, recognising that children may be present in the area.

Given the nature of the location and the purposes of crime prevention and public safety, individuals would reasonably expect surveillance to be in operation 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?

The surveillance camera system will be configured and operated strictly for its stated lawful purposes of crime prevention, public safety and the reduction of anti social behaviour. Camera positioning and fields of view are limited to the Jubilee Hall entrance and fire exit only, capturing no more data than is necessary to achieve these purposes and avoiding private areas wherever practicable.

Only relevant video and audio data will be recorded, with no use of analytics, facial recognition, profiling or automated decision making. Access to live and recorded footage is restricted to authorised and trained personnel, and recordings are retained for a limited and defined period before automatic deletion, unless required for a specific lawful purpose such as an investigation.

Compliance and effectiveness will be supported through regular review of system use, incident logs, improved site management, or successful investigation of incidents when they occur. The continued use of the system will be kept under review to ensure it remains necessary, proportionate and effective in delivering its intended benefits.

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

Footage is retained for 30 days and then automatically deleted unless stored. This should give investigating authorities and Data Subjects sufficent time to request footage Please see below.

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)

Footage may be retained for more than 30 days. e.g. major incident where a large amount of data has been retained for investigation. Civil Proceeddings and Subject Access Requests.

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?

Access is restricted to the room and system. The system is password protected. DVD's or encrypted USBs are released to police officers and to third parties such as Insurance companies and solicitors via recorded delivery and email confirmation prior to disclosure of the encryption code. No international transfers are made.

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 councils CCTV policies and procedures are fully compliant with the GDPR/DPA 2018 for general disclosure access requests and CCTV related subject access requests. Information on subject access can be found on the Cayton Parish Council website and all requests are initially dealt with by the Parish Clerk.

Any complaints are dealt with through the councils complaints procedures.

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)

Any operation to do with CCTV is audited. This includes the use of cameras, reviewing and downloading images, access, storage and incidents recorded.

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**
Non Compliance of GDPR/DPA 2018. The GDPR/DPA sets out seven key principles which LA CCTV System owners must comply with whilst operating a Public Space Surveillance System: • Lawfulness, fairness and transparency • Purpose limitation • Data minimisation • Accuracy • Storage limitation • Integrity and confidentiality (security) • Accountability Non compliance may result in prosecution,financial penalties and severe damage to the reputation of the local authority	Remote, possible or probable Possible	Minimal, significant or severe Minimal	Low, medium or high Low
Compliance with articles 6, 8 and 14 of the Human Rights Act.The Act applies to public authorities and other bodies, which may be public or private, when they are carrying out public functions Article 6: the right to a fair trial Article 8: right to a private and family life Article 14: protection from discrimination Possible Significant Medium	Possible	Significant	Medium

Compliance with SC Code of Practice and the Protection of Freedoms Act 2012. The code of practice is issued by the Secretary of State under Section 30 of the 2012 Protection of Freedoms Act. Relevant authorities (as defined by section 33 of the 2012 Act) in England and Wales must have regard to the code when exercising any functions to which the code relates. A failure on the part of any person to act in accordance with any provision of the surveillance camera code does not of itself make that person liable to criminal or civil proceedings. The surveillance camera code is admissible in evidence in any such proceedings. (A court or tribunal may, in particular, take into account a failure by a relevant authority to have regard to the surveillance camera code in determining a question in any such proceedings. This is reflected in the Crown Prosecution Service Disclosure Manual Reputational damage to Local Authority. The court may take inference in an authorites non compliance.	Possible	Significant	Medium
Security of Data. A Security Data breach may result in prosecution under GDPR/DPA 2018 and result in financial penalites and severe damage to the reputation of the local authority	Possible	Significant	Medium
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**
Unauthorised Disclosure Unauthorised Disclosure may result in prosecution under GDPR/DPA 2018 and subject to financial penalites and severe damage to the reputation of the local authority	Remote, possible or probable Possible	Minimal, significant or severe Significant	Low, medium or high Medium

Misuse of Data Misuse of data may result in prosecution under GDPR/DPA 2018 and subject to financial penalites and severe damage to the reputation of the local authority	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?**
Compliance with GDPR/DPA 2018. Management of the use and security of the system including monitoring, reviewing and downloading of footage. Which includes a record kept of each access by whom and with whom present.	Eliminated reduced accepted Reduced	Low medium high Low	Yes/no Yes
Compliance with articles 4, 6 and 13 of the Human Rights Act Management of the use and security of the system including monitoring, reviewing and downloading of footage. Spot checks on proactive monitoring by staff.	Reduced	Low	Yes
Compliance with SC Code of Practice and the Protection of Freedoms Act Management of system.	Reduced	Low	Yes

Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved?
Security of Data Management of the use and security of the system including monitoring, reviewing and downloading of footage.	Eliminated reduced accepted Reduced	Low medium high Low	Yes/no Yes
Unauthorised Disclosure Release of data is strictly controlled by the council. All parties who use data from the system are aware of their obligations under GDPR/DPA. Full audit trail for any release of data. Staff trained in unauthorised disclosure and misuse of data.	Reduced	Low	Yes
Misuse of Data Release and use of data is strictly controlled by the council. All parties who use data from the system are aware of their obligations under GDPR/DPA. Full audit trail for any release of data. Staff trained in unauthorised disclosure and misuse of data.	Reduced	Low	Yes
Financial Loss. Compliance with GDPR/DPA, POFA, Code of Practice and operating procedures reduces the risk of unauthorised disclosure or the misuse of data.	Reduced	Low	Yes

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:	Full Council	Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by:	Full Council	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: DPO and reviewed by Full Council each year.		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)
Jubilee Hall			24hrs on motion	N/A	The privacy level expectation in a public building is low; the building is well signed with appropriate signage for CCTV its use and purpose with contact details.

Date and version control: 19 May 2020 v.4

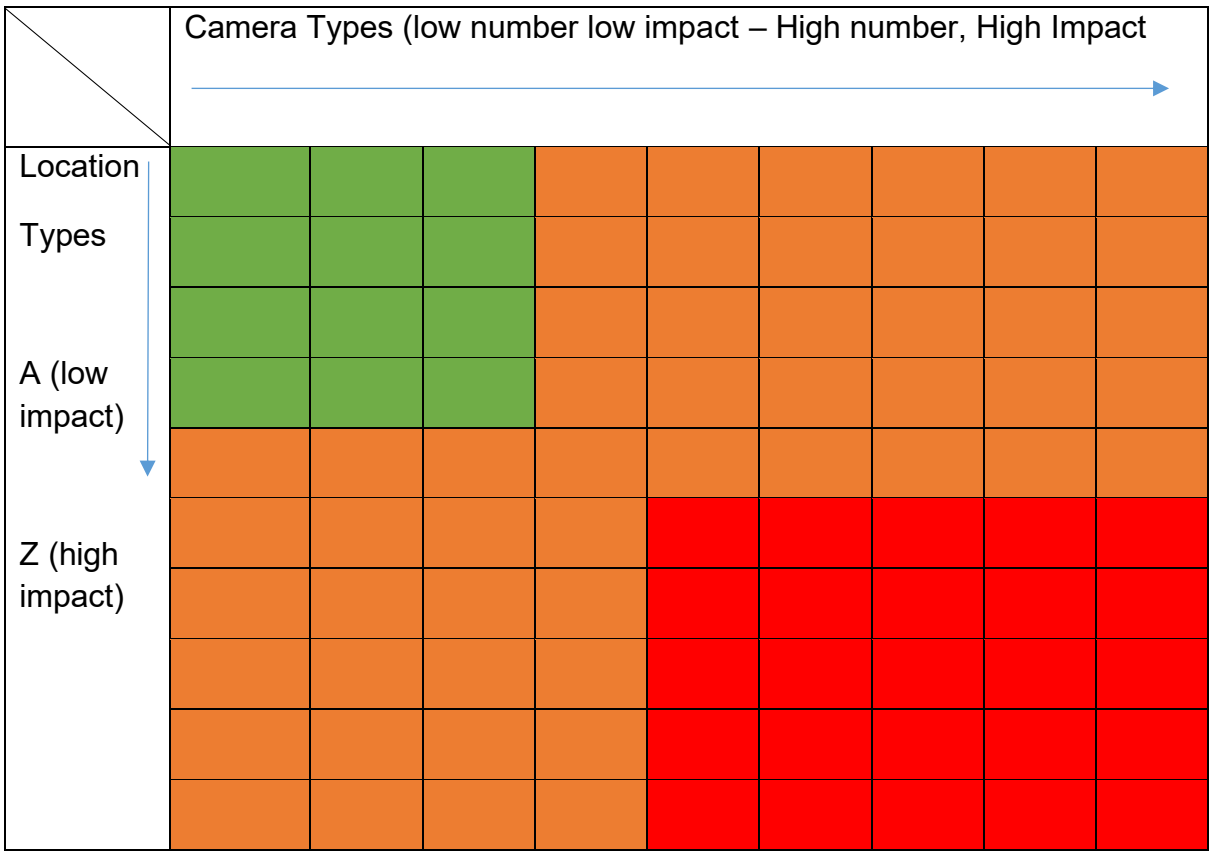
APPENDIX TWO: STEPS IN CARRYING OUT A DPIA

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