



**SURVEILLANCE CAMERA  
COMMISSIONER**

**ico.**  
Information Commissioner's Office

APPENDIX 1

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



## Project name: Waterside Bridge (2 x pan and tilt cameras and a help button)

### 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<sup>1</sup>:

- |   |   |
|---|---|
| <input type="checkbox"/> Systematic & extensive profiling | <input type="checkbox"/> Large scale use of sensitive data        |
| <input checked="" type="checkbox"/> Public monitoring     | <input type="checkbox"/> Innovative technology                    |
| <input type="checkbox"/> Denial of service                | <input type="checkbox"/> Biometrics                               |
| <input type="checkbox"/> Data matching                    | <input type="checkbox"/> Invisible processing                     |
| <input checked="" type="checkbox"/> Tracking              | <input type="checkbox"/> Targeting children / vulnerable adults   |
| <input type="checkbox"/> Risk of harm                     | <input type="checkbox"/> Special category / criminal offence data |
| <input type="checkbox"/> Automated decision-making        | <input type="checkbox"/> 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)?

This is a new development. It is the construction of a pedestrian and cycle bridge across the River Trent. A drawing is provided to assist with understanding the location. We will be processing under DPA 2018.

### 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.

There is no evidence of crime statistics as this is a new construction. Areas to the Northside are relatively new developments also, and there is currently no access from the South side to the North.

Reasons for installation of the help button and 2 x CCTV cameras are to monitor and assist with the risk of suicide, and also to prevent anti social behaviour and vandalism of the new bridge structure. The Suicide prevention Officer asked that we consider this installation as part of the scope of works.

Neighbouring residents also requested this installation as part of a consultation in 2023.

<sup>1</sup> <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?

The new bridge will be a public pedestrian and cycle route, used by people of all ages and ethnicities.

Adjustments will be made to the images recorded to ensure that neighbouring properties continue to have privacy within their homes.

These cameras are likely to be located at each end of the bridge and will be a permanent fixture. They will be in place to prevent vandalism and anti social behaviour.

**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.

Nottingham City Council will make decisions regarding footage in conjunction with the Legal Team and Police for the prevention and detection of crime.

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

- |  |   |
|--|---|
| <input checked="" type="checkbox"/> Fixed CCTV (networked) | <input type="checkbox"/> Body Worn Video                  |
| <input type="checkbox"/> ANPR                              | <input type="checkbox"/> Unmanned aerial systems (drones) |
| <input type="checkbox"/> Stand-alone cameras               | <input type="checkbox"/> Redeployable CCTV                |
| <input checked="" type="checkbox"/> Other (please specify) |   |

Help button.

**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.

See the data flow mapping and the Information Asset register. No audio will be recorded. There will be no automatic facial recognition used.

All staff operating the cameras are UK GDPR trained on an annual basis and also receive RIPA and information security training

**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.

Woodlands Control Room

**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   |
|----------------------------------|---------------------|--------------|--|
| Blueprint and Management Company | Teams meeting       |              | Agreed installation to protect asset, reduce anti-social behaviour, and provide support and assistance via help button |
| Trent Basin Residents            | Email               |              | Agreed installation to protect asset, reduce anti-social behaviour and provide support and assistance via help button  |

## 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 under Article 6 of the UK GDPR is 1(e) that the processing is necessary for the performance of a task carried out in the public interest or the exercise of official authority vested in the controller. It is not expected that the CCTV would specifically capture any special data but if it did it would be covered by Article 9-2 (g) namely that the processing would be necessary for reasons of substantial public interest. The camera is installed for prevention of crime purposes in accordance with our fair processing notice.

**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.

People in public places will be made aware of the signage. Such awareness on the part of the public supports and informs the concept of surveillance by consent.

If the signage was not in place there would be a risk that citizens would not know they were under surveillance which would be an intrusion to their privacy.

**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?

Cameras should not be used to infringe an individual's right to privacy unless it is both necessary and proportionate. There must be an appropriate balance between public protection and individual privacy. There is a risk that privacy could be infringed by the use of camera's, especially if the use is not necessary and proportionate. There will be no audio or facial recognition thereby lowering the risk of intrusion to privacy. Camera footage will only be examined when an incident has occurred or for criminal investigations.

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

Recordings will be kept in line with NCC's retention period - 31 days.

There are strict processes in place to limit the viewing of live and recorded images to those for a lawful purpose and with the appropriate level of authority and only with a legitimate reason.

#### **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 cameras have been purchased to ensure sufficient quality and to ensure that they are fit for purpose to prevent and detect crime and to ensure public safety. There is an annual review of these cameras to ensure that they continue to meet current and future needs. A Secure control access is restricted to authorised personnel only

**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.

There are strict rules relating to any wider use of images, and our CCTV Policy, our Data Protection Policy, and Operational Guidance stipulate what use can be made of the CCTV.

The information compliance team work in conjunction with the CCTV team to ensure all lawful requests are actioned according to the UK GDPR and DPA 2018. Operational Guidance stipulates what use can be made of the CCTV. Any requests will be refused unless a lawful exemption applies

**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.

Patrol by Community Support Officer - limited resource to address vandalism.  
Improved lighting - not taken forward as it is thought that this would more vandalism to the area, as they would be encouraged to hang out in the undercroft after dark.



**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)

Disclosure, Production, Accessed, Handled, Received, Store 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.

| <b>Describe source of risk and nature of potential impact on individuals.</b> Include associated compliance and corporate risks as necessary.   | <b>Likelihood of harm</b>    | <b>Severity of harm</b>        | <b>Overall risk</b> |
|---|------------------------------|--------------------------------|---------------------|
| <p>1. Cameras should not be used to infringe an individual's right to privacy unless it is both necessary and proportionate. There must be an appropriate balance between public protection and individual privacy. There is a risk that privacy could be infringed by the use of cameras, especially if the use is not necessary and proportionate.</p> <p>2. The cameras are focused on the open space. People in public places will be made aware by the signage.</p> <p>3. There is a risk that privacy may be curtailed as citizens do not realise they are being filmed by CCTV.</p> <p>4. There is a risk that data will be kept too long which would be in breach of the data protection principle of data minimisation.</p> <p>5. There is a risk that too many staff at Nottingham City Council would have access to the footage and could disclose the footage to others outside NCC without a lawful reason to do so.</p> | Remote, possible or probable | Minimal, significant or severe | Low, medium or high |
|   | Remote                       | Minimal                        | Low                 |
|   | Remote                       | Minimal                        | Low                 |
|   | Remote                       | Minimal                        | Low                 |
|   | Remote                       | Minimal                        | Low                 |
|   | Remote                       | Minimal                        | 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.**

| <b>Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk</b>   |                                   |                      |                          |
|---|-----------------------------------|----------------------|--------------------------|
| <b>Options to reduce or eliminate risk</b>  | <b>Effect on risk</b>             | <b>Residual risk</b> | <b>Measure approved?</b> |
|   | Eliminated<br>reduced<br>accepted | Low medium high      | Yes/no                   |
| 1. There will be no audio or facial recognition as this will be configured not to detect when commissioned. Thereby lowering the risk of intrusion to privacy. A full DPIA will be carried out for each new camera or groups of cameras if placed in close proximity. | Accepted                          | Medium               | Yes                      |
| 2 If the signage was not in place there would be a risk that citizens would not know they were under surveillance which would be an intrusion to their privacy.   | Accepted                          | Low                  | Yes                      |
| 3. The recording will be kept in line with NCC's retention period   | Accepted                          | Low                  | Yes                      |
| 4. There are strict processes in place to limit the viewing of live and recorded images to those for a lawful purpose and with the appropriate level of authority and only with a legitimate reason.  | Accepted                          | Low                  | Yes                      |
| 5. Privacy masking will be used on cameras overlooking residents properties   | Accepted                          | 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.

| <b>Item</b>  | <b>Name/date</b>  | <b>Notes</b>   |
|--|---|--|
| Measures approved by:  | Sam Cooper<br>Security and Logistic Officer<br>27/01/2023 | Integrate actions back into project plan, with date and responsibility for completion.   |
| Residual risks approved by:                                  | Sam Cooper<br>Security and Logistic Officer<br>27/01/2023 | 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:<br>(specify role/title) |   | If overruled, you must explain your reasons.   |
| Comments:  |   |  |
| Consultation responses reviewed by:                          | Helen Wallace<br>Project Manger                           | If your decision departs from individuals' views, you must explain your reasons.   |
| Comments:  |   |  |

|   |                                 |  |
|---|---------------------------------|--|
| This DPIA will be kept under review by: | Helen Wallace<br>Project Manger | The DPO should also review ongoing compliance with DPIA. |
|---|---------------------------------|--|



## 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) |   |  |  |  |  |  |  |  |  |  |
|                 |   |  |  |  |  |  |  |  |  |  |
|                 |   |  |  |  |  |  |  |  |  |  |
|                 |   |  |  |  |  |  |  |  |  |  |
|                 |   |  |  |  |  |  |  |  |  |  |