

Data protection impact assessment

Drone surveillance pilot- Burnley Council

February 2025



Project name: Back Street Flytipping Drone Pilot

Data controller(s): Burnley 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 DPIA¹:

- | | |
|---|---|
| ☐ 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) |

The intention is monitor dirty back yards and to assess whether items that have accumulated in private property ends up being illegally flytipped on the public highway. While there is no intention to systematically monitor individuals, there is a small chance that the surveillance will catch an individual in the act of flytipping. The individual will be tracked to a property if possible within the constraints of the regulations for drone flight.

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)?

- UK GDPR applies because drone footage may capture identifiable individuals, properties, or vehicles, making it "personal data."
- DPA 2018 provides specific lawful bases for processing, particularly where public task or law enforcement purposes (such as fly-tipping enforcement) are involved.

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 project aims to reduce the incidence of flytipping in a targetted area of Bankhall ward (around Leyland Road) by monitoring waste build up using a camera drone.

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?

The drone footage will capture images and videos of backstreets, yards, and waste deposits. It may incidentally record identifiable individuals, vehicles, or property.

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.

Rob Dobson, Chief Operating Officer.
The data processor for the council is Skyfarer. Skyfarer.co.uk

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.

The images will be captured to a secure server by Skyfarer.
The images will remain on the Skyfarer server until the project has completed (no more than 12 months).
The images will then be permanently deleted from the Skyfarer service but examples containing no personal information may be retained by the council.
No integrated surveillance technologies will be used.
Images of flytipping or similar maybe retained for longer to enable the appropriate action to take place.

8. Does the system's technology enable recording?

☒ Yes X ☐ 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.

At Skyfarer 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
Ward Councillors in pilot area	Email	Supportive	
Executive Members	Email and meetings	Supportive	

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.

- UK GDPR Article 6(1)(e) - Public Task (Processing is necessary for a task carried out in the public interest)
- UK GDPR Article 6(1)(f) - Legitimate Interests (Where applicable, balancing the interests of the council and public with individuals' rights)
- Data Protection Act 2018 - Part 3 (Where processing may involve law enforcement purposes)

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.

Notices in area under surveillance. Information on the council's website.

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?

Drones will focus on capturing waste disposal areas, not individuals.
Images quality will be too low to able identify an individual's face.
Data will be reviewed to remove any unnecessary personal data before further processing.
There will be no ancillary uses of the data, such as to capture illegal parking or abandoned vehicles.

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

Less than 12 months. See next section.

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)

Data on the Skyfarer system to be deleted automatically.
Data on council server's to be deleted manually after enforcement/engagement action.
Non-personal information may be stored indefinitely as part of a project lesson learnt report.

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?

Footage stored on secure, access-controlled servers.
Data will be transferred from the data processor to the council securely using TLS (version 1.2 or above)
Restricted access to authorised officers.
Encryption used where necessary.

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 council has an established process for handling subject access requests. Residents can contact the council's Data Protection Officer to:

- Request access to footage containing their image.
- Object to processing if they believe it infringes their rights.
- Request deletion of footage (subject to legal constraints).

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.

The council has identified persistent illegal waste dumping in certain areas. Drone surveillance provides a cost-effective and efficient method of assessing the scale of the issue and supporting targeted enforcement.

Alternative methods (e.g., manual inspections) have been considered and are used, but are resource-intensive and potentially less effective for gathering comprehensive evidence over a wide area.

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)

The council has established policies and procedures in place for SARs and data protection. The council's internal audit team provides independent audit and assurance but given the time limited nature of this project and the risk to personal information, this is not considered necessary on this occasion.

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
Capture of identifiable individuals	Remote, possible or probable Possible	Minimal, significant or severe Minimal	Low, medium or high Medium
Unauthorised access to drone footage	Remote	Minimal	Low
Retention of footage beyond necessity	Remote	minimal	Low
Public concerns over privacy	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
	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?
Capture of identifiable individuals: Cameras set to focus on waste areas; signs displayed notifying residents. Flight distance to ground likely high enough to reduce the risk	Eliminated reduced accepted Reduced	Low medium high Low	Yes/no Yes
Public concerns over privacy: public communication and engagement before flights	Accepted	Medium	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: COO	Rob Dobson, 11/02/2025	Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by: COO	Rob Dobson, 12/02/2025	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:	Ian Evenett, 12/02/2025	DPO should advise on compliance and whether processing can proceed.
Summary of DPO advice Need to consider the transference of Fly Tipping images to the Council from the processor – details of how this will be securely transferred. Also need to consider the retention periods for these. Need to be clear that ancillary use will not be used – illegal parking, abandoned vehicles etc.		
DPO advice accepted or overruled by: COO (specify role/title)	Rob Dobson	Accepted
Comments: Updated in light comments.		
Consultation responses reviewed by: COO	Rob Dobson, COO	If your decision departs from individuals' views, you must explain your reasons.
Comments:		

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

APPENDIX ONE- NOT USED

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)

APPENDIX TWO: STEPS IN CARRYING OUT A DPIA



APPENDIX THREE: DATA PROTECTION RISK ASSESSMENT MATRIX- NOT USED

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)										

NOTES

