



**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:** Body Worn Cameras for Broads Authority Front Line Staff

**Data controller(s):** Rob Rogers (Data Protection Officer)

**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 type="checkbox"/> Tracking                         | <input type="checkbox"/> Targeting children / vulnerable adults              |
| <input checked="" type="checkbox"/> Risk of harm          | <input checked="" type="checkbox"/> Special category / criminal offence data |
| <input type="checkbox"/> Automated decision-making        | <input checked="" type="checkbox"/> Other (please specify)                   |

BWC recordings will take place in public areas and will pick up personal data from others and minors unrelated to the events being recorded.

**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 Broads Authority intends to run a BWC trial to assess the impact, effectiveness and perceptions of the BWC technology. We will trail 5 body worn cameras in different key locations within the Broads National Park area.

The trial will end on 30 August 2024.

The consultation period will close in September 2024.

Reporting to the Navigation Committee and The Broads Authority will take place in November 2024.

Information such as videos and audio recordings that can identify an individual are classified as personal data under the Data Protection Act 2018 (DPA 2018). Under the UK's implementation of the EU General Data Protection Regulations (GDPR) personal data must be processed consistent with seven data protection principles.

<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/>

## 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.

Personal Body worn cameras will be worn by Rangers and Quay Rangers at all times, the recording capability of the BWC will be used at the discretion of the wearer and used specifically for the purpose of law enforcement.

Lawful- processing of sensitive data for law enforcement purposes, is only lawful in two cases:

Case 1: There is:

- a) consent by the data subject for law enforcement purposes and
- b) at the time the data processing carried out the competent authority has an appropriate policy document in place.

Case 2:

- a) The processing is strictly necessary for law enforcement purposes and
- b) the processing meets at least one of the conditions in Schedule 8, and
- c) at the time when the processing is carried out, the controller has an appropriate policy document in place.

It is under Case two (2) that the Broads Authority BWC trial will take place.

Given enforcement scenarios or byelaw infringements, or abusive or threatening incidents (whilst undertaking enforcement duties) can occur at any time the cameras will be worn whilst staff are on duty.

Recording will be carried out overtly, with a verbal announcement made to the subject matter that "recording has been initiated for safeguarding purposes".

BWC will not be used for covert surveillance.

During the trial period recordings will be uploaded to a secure virtual storage area, with controlled and limited access, via Sharepoint for review.

The Review team will be the Director of Operations, DPO and the Senior Ranger Team or associated Senior Officers. Captured data during the trial period will be deleted on a week-by-week basis for basic captured images that require no further actions.

For data that is required for evidential reviews a retention period of seven years will be applied as per the Broads Authority Data Management Policy. Retained data needed for evidential purposes will follow the strict processes associated with PACE (Police and Criminal Evidence Procedure Act 1984) overseen by the Compliance and Enforcement Senior Ranger.

**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?

Personal data of visitors to the Broads National Park and residents, landowners, non-compliant boat owners and other third parties working or using Broads Authority waters, assets or surrounding land.

Under section 36(c) Personal data collected for a law enforcement purpose may be processed for any other law enforcement purpose by the controller “provided that—

- (a) the controller is authorised by law to process the data for the other purpose, and
- (b) the processing is necessary and proportionate to that other purpose”.

Processing – The data processed for law enforcement purposes must be adequate, relevant, and not excessive in relation to the purpose for which it is processed (s37)

Security – Data must be processed in a way that ensures adequate security is in place (s40).

The collection of this personal data and why is explained within the Body Worn Camera Policy.

**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 decision to turn on the BWC and record footage is at the discretion of the wearer (as per our policy). Once recorded data is downloaded it to the virtual laptop via the cloud, access to the data will be controlled by differing levels of access, all password protected.

Ranger captured data will be reviewed at the earliest opportunity by the Senior Ranger Team and the Operations Director with any footage linked to criminal acts being forwarded to the Police. For other Byelaw offences the review will follow existing prosecution protocols <https://www.broads-authority.gov.uk/about-us/how-we-work/legislation>

Data captured by the Quay Rangers will be reviewed by the Head of Visitor Services, The DPO and the Head of Communications, with actional footage following the above processes.

Data captured by Planning Enforcement will be reviewed by the Head of Planning , The DPO and The Authority's legal providers and follow planning law processes.

**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)

It is proposed to capture both video and audio recordings. Given the data is for law enforcement purposes the data must be adequate, relevant, and not excessive for the purpose (s37). Audio alone would not help identify the individual committing the breach of the byelaw, therefore video is adequate, relevant and not excessive.

**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.

For the BWC trial:

1. Data Captured on the D3 BWC after the wearer announces the recording has started.
2. Captured data will be downloaded onto Authority virtual and secure laptop and saved in a Sharepoint secure folder, via the Cloud secure storage facility. Access will be limited and controlled by level access and password authentication.
3. Non flagged files will be deleted in accordance to the Broads Authority Data Retention Policy.
4. Evidential files will remain securely stored, under a strict access policy.
5. Evidential files will be deleted in accordance to the Broads Authority Data Retention Policy or once they are no longer required.

Information such as videos and audio recordings that can identify an individual are classified as personal data under the Data Protection Act 2018 (DPA 2018). Under the UK’s implementation of the EU General Data Protection Regulations (GDPR) personal data must be processed consistent with seven data protection principles.

## 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.

Within the various locations with the Broads National Park or on land or waters managed by the Authority, recording will include audio and visual for the purpose of law enforcement.

## 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)

Secure data will be shared by password secured and pre-approval to the Sharepoint stored folder. Data will not be disclosed outside the Broads Authority unless its meets the GDPR & Data Protection exemptions

## 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)

Recorded data will be used to support byelaw enforcement, including speeding, care and caution and overstaying. As well as providing training examples for the front line staff development and for the production of warning letters and other communication material. If needed the data will be redacted to protect data subjects and comply with Data Protection and GDPR.

The camera record function will be turned on when Broads Authority staff are dealing with a prima facie breach of the byelaws, not when an incident starts to get heated, as this would exacerbate the situation.



## 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
Broads Authority Ranger Teams, Head of Communications, Management Team & Visitor Service Manager	Video conference discussions and feedback	Initial views reserved until trial period has concluded. Perceived issues around the public perception, staff concerns on video evidence being used to evaluate them and possible escalation of situations due to the BWC	All concerns and issues will be fully discussed and feedback reviewed once trial period ends.
Chairman of the Broads Authority	Verbal discussion with CEO	Supportive of measures designed to improve staff safety.	Board paper required following trial period to explore needs and benefits, costs and risks.



--	--	--	--

## 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.

Police and Criminal Evidence Act 1984 (PACE)  
The Human Rights Act 1998  
Regulation of Investigatory Powers Act 2000  
Data Protection Act 2018  
EU GDPR 2016/679  
Health and Safety at Work Act 1974  
Norfolk and Suffolk Broads Act 1988  
Broads Act 2009

Recordings will be made specifically for the purpose of safeguarding the health and safety of Broads Authority staff and the general public and for evidential purposes for byelaw enforcement, legal action or for the purposes of issuing warnings.

**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.

For the trial period staff will issue a verbal warning that evidential video is being captured, for the trial duration the Broads Authority Privacy Notice will be amended to reflect the BWC evidence and data retention.

**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?

Continuous recording will not take place.

Autonomous recordings will not be used.

BWC will be allocated to staff trained in handling difficult situations and trained in the appropriate use of the BWC technology.

BWC recording will be initiated by Broads Authority staff members on start of an interaction and cease at its conclusion.

BWC will be connected to a work provided laptop to facilitate encrypted upload to secure cloud storage.

Access to view or share the recordings will be restricted to the Management Team, Heads of Section and the Senior Ranger Team. All access to the protected files will be via appropriate authorisation and secure login.

Training provided to staff involved in the BWC project and refreshed periodically.

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

Non-flagged files (incident not deemed actionable) 30 days.

Evidential files needed for criminal evidence 7 years or in accordance to Data Retention Policy.

No data will be retained beyond its usefulness.

### 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 retention of BWC data will be specifically reviewed on a monthly basis by the DPO.

**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?

BWC data is automatically encrypted and access via the BWC is by a six digit pin number. BWC data will be downloaded onto a Broads Authority issued (approved and security & virus protected) laptop. Downloaded data will be stored in a restricted access Sharepoint secure folder. Once BWC D3 camera is downloaded the SIM card is auto deleted ready for additional camera data capture. Sharing of BWC data will be via the secure Sharepoint with controlled access.

**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.

All DSAR are issued to the DPO who will have access and owner rights to the BWC sharepoint folders. The DPO will ensure that the BWC data is included within the system search required under the DSAR. The Data Protection policy will be amended to reflect this change once the trial BWC period has ended and the BWC project continues to roll-out.

**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.

Extensive training of handling difficult situations, managing the public, Ranger shadowing to assist newer Ranger, Broads Authority policies of staff conduct.

Given the one on one interactions between staff and potential surveillance subjects, the remoteness of where some of the interactions take place and the need to protect staff, the BWC project is seen as a much needed added deterrent to abusive/violent behaviour and byelaw offences occurring within our managed landscape.

**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 Broads Authority's processes and procedures are internally audited by an approved auditor and we are also subject to external audits, on processes randomly selected.

We also carry out internal reviews if changes happen, following an incident or if legislation changes.



## 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>
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
Continuous or inappropriate covert recording	Possible	Significant	Low - staff trained to use camera. Trusted and professional staff, regular 1:1 and Line Manager Liasons.
Breach of data security	Possible	Significant	Low - Data Protection training regularly refreshed, Close ties to the DPO, good access to guidance and established protocols. Staff already work with high standards of data protection and knowledge of

			protecting personal data.
Loss or Theft of BWC	Possible	Significant	Medium - staff water based. Being worn at all times increases the risk of work duties knocking the camera from mountings. Authority reviewing mountings to obtain the most secure.
<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>
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
Unauthorised access, sharing or use of BWC data	Possible	Severe	Low - data protected on sharepoint limited access and passwords protected folder. Sharing would be via DPO only and using already bestablished secure sharing methods (limited ,

			Timed access via sharepoint)
Subjects not related to incidents being recorded	Possible	Severe	Low - Supplied software allows redaction of non-specific individuals or minors. No Shared data would be allowed until DPO reviewed and cleared the redactions and adherence to Data Protection & GDPR
Public perceptions of recorded data and safe use.	Possible	Medium	Low - existing data protection in place, robust procedures on deletion and retention, staff trained in data protection and GDPR



## 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 reduced accepted	Low medium high	Yes/no
Provide guidance to BWC users on appropriateness of use of the device. Ensure users are trained in appropriate use. Audit appropriateness of device use per user.	Reduced	Low	yes
Provide guidance to BWC users on appropriateness of use of the device. Ensure users are trained in appropriate use.  Audit appropriateness of device use per user.  In order to ensure all aspects of an incident are captured, this requires the inclusion of audio information in order for this to be complimentary to the video data. Sometimes the camera may not be pointing in the direction of the main incident but the audio will still be captured. This has a significant advantage of protecting all parties to ensure the actions of the Operational staff are totally in accordance	Reduced	Low	yes

with the law. Equally, the presence of only video evidence without the added context that audio, can fail to adequately provide the full context for all parties of an incident or interaction.			
<b>Options to reduce or eliminate risk</b>	<b>Effect on risk</b>	<b>Residual risk</b>	<b>Measure approved?</b>
	Eliminated reduced accepted	Low medium high	Yes/no
Review recordings to retain only those recordings required in line with Authority policy. Edit or obscure sections of the recording if they identify individuals who are not the subjects of concern.	Reduced	Low	yes
Ensure movement of devices is monitored and they is a checking in/out process.  A device may become detached and fall into unauthorised possession, although provided encryption is enabled it should not be possible for the data to be accessed by an unauthorised individual.  Where a device is lost, all possible attempts will be made to identify and notify persons who are subjects of information on the device	Reduced	Low	yes
In the event that a subject matter requests that the BWC be switched off, they should be advised that: • Any non-evidential material is retained for 30 days. • This material is restricted and cannot be disclosed to third parties without the express authority of the subject of the recording unless prescribed by law.	Reduced	Low	yes

Ensure the purpose for the activation of the recording features of the devices does not change and remains within the legal basis for processing

Reduced

Medium

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:		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:		The DPO should also review ongoing compliance with DPIA.
---	--	--

## 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)

## APPENDIX TWO: STEPS IN CARRYING OUT A DPIA



## APPENDIX THREE: DATA PROTECTION RISK ASSESSMENT MATRIX

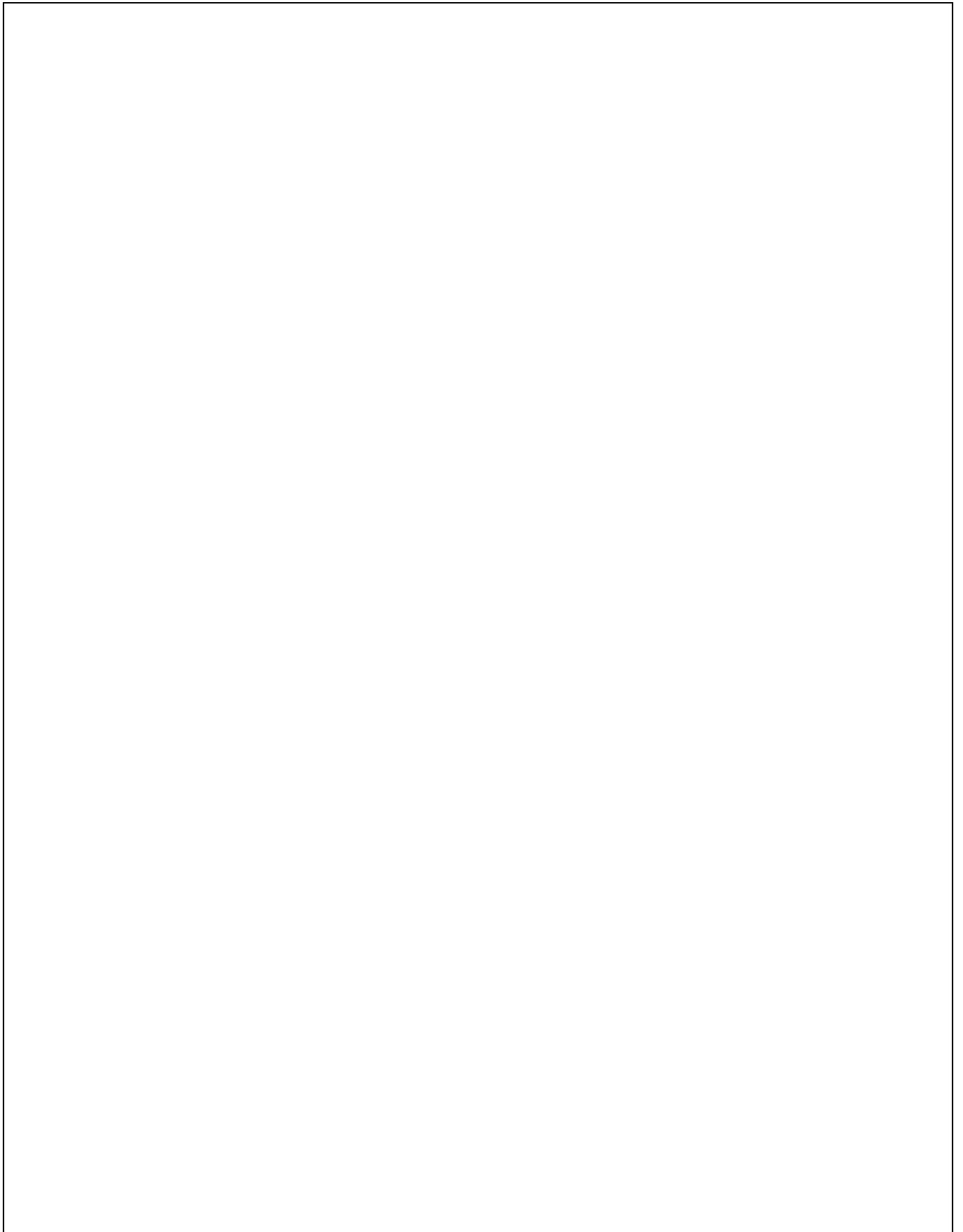
Use this risk matrix to determine your score. This will highlight the risk factors associated with each site or functionality.

### Matrix Example:

	Camera Types (low number low impact – High number, High Impact)								
Location									
Types									
A (low impact)									
Z (high impact)									



## NOTES

A large, empty rectangular box with a thin black border, occupying most of the page. It is intended for handwritten or typed notes.

Date and version control: 19 May 2020 v.4

