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 DNPA Ranger Service

Data controller(s): Ali Bright (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[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)

Use of BWC by Rangers will by default record personal information of visitors to Dartmoor and other third parties that the Rangers have dealings with on a day to day basis

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)?

DNPA intends to deploy Reveal DEMS360 D3 body cameras to all 11 members of its Ranger team in March 2022.

Data will be processed in accordance with Data Protection legislation (including the Data Protection Act 2018 and EU GDPR 2016/679)

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 issue BWC will be worn by all members of the Ranger Service when attending particular sites or situations that may present a higher risk.
Rangers will have discretion to use personal issue BWC at any other sites, if they choose to do so.
Recordings will be made specifically for the purpose of safeguarding the health and safety of Ranger Team members and general public and for evidential purposes for byelaw enforcement and other legal action.

[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/

Recording will be initiated when the Rangers become involved in interactions with the general public, and must be carried out overtly. No covert survillance is to be carried out using personal issue BWC. Recordings will be uploaded to Reveal's secure cloud infrastucture and automatically deleted as detailed in the Authority's Data Retention schedule.

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 information relating to visitors to Dartmoor and other third parties that the Rangers have dealing with on a day to day basis.

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.

Members of the Ranger Team will overtly initiate recording when entering an interaction with members of the public or conducting interviews under caution with any person relating to byelaw offences for which they may be reported for court action.

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.

Capture
Connect camera to work provide Laptop with Reveal DEMS360 software installed
Upload to Reveal secure cloud (files for evidential retention flagged)

Non flagged files auto deleted in accordance with the Authority's Data Retention Schedule.
Evidential files retained on Reveal cloud with access strictly controlled.
Evidential files deleted in accordence with the Authority's Data Retention Schedule

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.

On site with audio and visual recording

9. If data is being disclosed, how will this be done?

☐ Only by on-site visiting

☐ Copies of footage released (detail method below, e.g. encrypted digital media, via courier, etc)

☒ Off-site from remote server

☐ Other (please specify)

10. How is the information used? (tick multiple options if necessary)

☐ Monitored in real time to detect and respond to unlawful activities

☐ Monitored in real time to track suspicious persons/activity

☐ Compared with reference data of persons of interest through processing of biometric data, such as facial recognition.

☐ Compared with reference data for vehicles of interest through Automatic Number Plate Recognition software

☐ Linked to sensor technology

☐ Used to search for vulnerable persons

☐ Used to search for wanted persons

☒ Recorded data disclosed to authorised agencies to support post incident investigation, including law enforcement agencies

☐ Recorded data disclosed to authorised agencies to provide intelligence

☒ Other (please specify)

Recorded data used to support byelaw enforcement or other legal action through warning letters as well as prosecution through the single justice process

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
Dartmoor National Park Authority Ranger Team	email and verbal	7 responses from 10 team members consulted (6 in favour; 1 against). Comments related to where/when/how filming would take place; having some discretion over use	Ranger Team Manager discussed issues with individual Rangers. Revised approach to be piloted requiring BWC to be used at specific locations where past records/experience have identified issues when engaging with the public. Rangers will have discretion whether to use BWC at other sites.
Unison	email (26/04/21). Ongoing dialogue with UNISON will be maintained, including Joint Staff Forum meetingheld on 15/02/22.	None	None.

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
Dartmoor Commons Act 1985
Common Law

Recordings will be made specifically for the purpose of safeguarding the health and safety of Ranger Team members and general public and for evidential purposes for byelaw enforcement and other legal action.

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.

Ranger Team vehicles prominently marked with appropriate signage relating to BWC
Cameras overtly worn by Ranger Team and clearly visible at all times
Ranger Team members explaining to public that BWC recording is taking place
Rangers Privacy Notice updated

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
BWC recording will be initiated by Ranger Team members on start of an interaction and cease at its conclusion.
BWC will be connected to a work provided laptop to facilitate encryped upload to secure Reveal cloud storage
Ranger Team members will have no access to view or share the recordings
Training provided to all Ranger Team Members prior to use, and refreshed periodically.

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

Non flagged files will be auto deleted after 30 days
Flagged files retained for evidence will be retained for as long as necessary or 3 years maximum in accordance with DNPA data retention schedule.

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 Controller supervises retention of materials held in support of prosecutions.

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 individually issued to and managed by each member of Ranger Team
All footage will be automaticaly encrypted, and only uploaded to the secure Reveal Cloud after connecting the camera to a work provided laptop with the Reveal360 software installed
Legitimate sharing of data will be by secure encrypted link shared from the Reveal Cloud by the Data Controller.

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.

In accordance with published DNPA policies.
https://www.dartmoor.gov.uk/about-us/how-we-work/open-data/freedom-of-information

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.

Ranger Team are experienced and trained in dealing with the public and managing conflict
BWC recording will not be continuous
Policy for Operation of BWC to ensure appropriate use, limit intrusion appropriately

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)

In accordance with published Data Privacy Notices
https://www.dartmoor.gov.uk/about-us/how-we-work/open-data/freedom-of-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.

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** Remote, possible or probable	**Severity of harm** Minimal, significant or severe	**Overall risk** Low, medium or high
Inappropriate or continuous recording.	Possible	Minimal	Low
Inability to switch off visual or audio recording.	Possible	Minimal	Low
Holding excessive recordings due to inappropriate or continuous recording on scene.	Possible	Minimal	Low
Loss/theft of camera.	Possible	Minimal	Low

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Unauthorised copying of footage to a personal device..	Remote	Severe	Low
Individual may object to being recorded.	Probable	Significant	Medium
The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge..	Probable	Significant	High
Public distrust about how information is used can damage an organisation's reputation..	Probable	Significant	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** Eliminated, reduced or accepted	**Residual risk** Low, medium or high	**Measure approved?** 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 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.	Reduced	Low	Yes

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
Ensure movement of devices is monitored and they is a checking in/out process.	Eliminated	Low	Yes
In the event that someone 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	Medium	Yes
Ensure the purpose for use 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.

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by:		If you identify a high risk that you cannot mitigate adequately, you must consult the ICO before starting to capture and process images.
DPO advice provided by:		DPO should advise on compliance and whether processing can proceed.
Summary of DPO advice : Processes in place cover identified risks and adequately mitigate any risks. Suitable training on the use of Body Worn Cameras including GDPR training must be given to all staff using them and evidence that each officer has undertaken the training must be recorded on their individual training files. Procedures, training content and risks must be reviewed regularly - recommend each quarter in the first year of implementation as a minimum - and incident log must be provided where members of the public object to the use of Body Warn Cameras. Any lessons to be learned must be considered and this DPIA reviewed/reassessed in light of experience.		
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.

Date and version control: 19 May 2020 v.4

Comments:		
This DPIA will be kept under review by: DPO and Ranger Team Manager		The DPO should also review ongoing compliance with DPIA.

Date and version control: 19 May 2020 v.4

APPENDIX ONE

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

Location: Each system operator/owner should list and categorise the different areas covered by surveillance on their system. Examples are provided below.

Location type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)

Date and version control: 19 May 2020 v.4

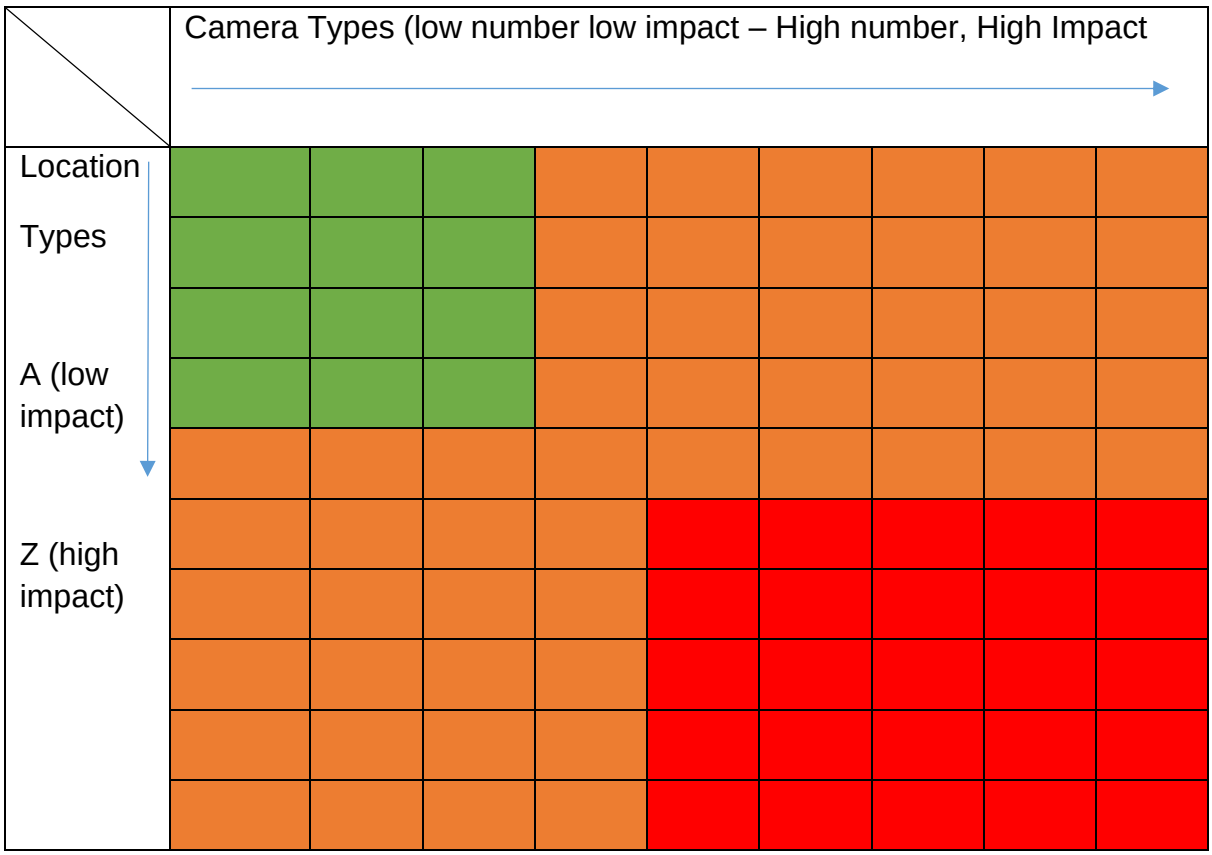
APPENDIX TWO: STEPS IN CARRYING OUT A DPIA

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