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: Blackpool Council - Public Protection and Enforcement - Body Worn Video Cameras

Data controller(s): Blackpool Council - ICO Registration: Z5720508

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)

Deployment of surveillance cameras is to safeguard staff and members of the public and to provide evidence for all parties in the event of any investigation into incidents, accidents or alleged assaults. Information will be collected using BWC cameras that will record images and sound of any interactions between the Blackpool Council's Public Protection Officers / Civil Enforcement Officers (CEO) and members of the public whilst undertaking parking enforcement operations and public protection enforcement actions.

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 Council primarily processes personal data from its CCTV network under the UK General Data Protection Regulation (GDPR), Article 6(1)(e) public task. This basis is underpinned by the Health and Safety Act 1974 which requires the Council to protect persons at work against risks to health or safety arising out of or in connection with activities at work.

There is also a raft of legislation supporting the enforcement action being taken which includes but is not limited to:

- Antisocial Behaviour, Crime and Policing Act 2014
- Consumer Credit Acts 1974 and 2006.
- Consumer Protection Act 1987.
- Consumer Protection from Unfair Trading Regulations 2008
- Criminal Justice Acts 1988 and 1991
- Criminal Justice and Police Act 2001
- Environmental Protection Act 1990
- Food Safety Act 1990 **
- Food Safety and Hygiene (England) Regulations 2013 **
- Health and Safety at Work etc Act 1974 **
- Housing Acts 1985 (as amended) , 1996, 1998, and 2004
- Pollution Prevention and Control Act 1999

[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/

The Data Protection Act 2018, Part 3 allows Blackpool Council to act as a competent authority (where it has the powers to do so) to process personal data (including special category data) for the prevention, detection or prosecution of criminal offences.

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.

Context – CCTV and body worn video are both in regular usage by agencies ranging from Police through to private agencies such as bailiffs, as such it is generally accepted by members of the public as a legitimate tactic. The use Of BWV by these agencies significantly reduces threat levels in confrontational situations. In addition it improves outcomes when used as an evidential tool. The decision whether to record or not will rest with the individual officer who, will be best placed to make a dynamic judgement as the situation develops.

Purpose - The use of BWV by the Public Protection Department is primarily to assist in the collection of evidential material for use in both civil and criminal enforcement cases.
Secondary considerations are the reduction in the fear of crime and providing reassurance to the public.
Maintaining the security and safety of staff engaged in enforcement activities.
Reduce the incidence of potentially confrontational incidents.

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?

Nature - The system records video and audio of anyone within the field of view when a body worn video device is activated. It has the potential to capture live images of people and anything they may say. The system is reactive to individual situations where body worn video is used and it will not be used to gather large amount of data (for example it will not be used to record during an entire day while a staff member is working)

Scope - The data subjects will be anyone the staff member feels they need to record with appropriate use of the body worn video device. If a recording is activated it will be stopped once a specific situation or incident has ended.

All recorded images and audio on a body worn video device stay on the device until it is placed into a docking station to upload. Docking stations are located in secure working environments controlled by the Council. Each staff member using body worn video is issued their own account on a Digital Evidence Management System. Unless marked as evidential all recordings are automatically deleted after 31 days. Evidential recordings are retained for a period of up to 2 years. Data on body worn video

devices is automatically deleted from the device after uploading. The system does not use facial recognition technology or have live streaming.

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.

Disclosure of information will only be done when compliant with applicable legislation and data sharing agreements will be in place to reflect routine processing. Blackpool Council regularly share CCTV image with the following organisations:

- Police,
- Legal Services

Any amendments to the processing outlined in this assessment will only be done with the approval of the Senior Responsible Officer (SRO) and Data Protection Officer (DPO)

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 use of BWV is primarily aimed at the capture of images and audio* in connection with the enforcement activities of the department's Civil Enforcement Officer's. Data processed will be include members of the public and Council staff.

The process briefly comprises of:

- Body cameras are dispatched from the office.
- Each camera is numbered from 1 to 21 for CEO's to use.
- A signing out sheet is used, linking to each cameras allocation.
- Activation is via a trained system operator who is responsible for the control of the BWV use and the processing of images and audio recording.
- Recording is manually activated by pressing the BWV's warning audio button.
- Members of the public are verbally advised when the body camera recording has been activated.
- The body camera will also light up red when in use.
- Once the member of the public walks away, the body camera is de-activated.

- The body camera is not activated during general public interactions and footage is not continuously recorded in order to reduce privacy concerns and is only activated when there is appropriate cause.
- Once activation has occurred, and on returning to the office, a decision will be made regarding footage download.
- Body cameras are placed within docking stations in dispatch to allow for the footage to be downloaded.
- Images and audio will be stored on a designated Council computer, held securely in the dispatch office which are held on secure Council servers.
- Retention of data is in accordance with the Council's overarching retention policy.
- Body cam footage will be held for 6 months. After this time and if no challenges have been received the footage will be deleted.
- Access to the saved footage is access controlled linked to role specific staff members such as the Head of Service and the Civil Enforcement Officer Supervisors (x2).

*Audio recordings and linkable data will consist of:
- The vehicle's registration number (VRN) aka number plate
- The street location

This is to allow the CEO in the event of an incident and no Penalty Charge Notice (PCN) being issued the ability to register linkable personal data to the relevant data subject.

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.

BWV Devices - Docked within Blackpool Council Public Protection and Enforcement Dispatch Office.

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
Council Officers	Meetings, emails, working group	Views raised on preferred purposes and methods	Considered as part of continued use.
Elected Members	(Audit and Scrutiny)	Views raised on preferred purposes and methods	Considered as part of continued use.
Police	Meetings, emails, working group	Views raised on preferred purposes and methods	Legitimate / Lawful access establish before sharing. Data shared using appropriate technical and organisation measures in place.
Staff	Meetings	Personal privacy could be compromised. May in-flame situations rather than de-escalate.	BWC procedure developed, distributed and adopted.
Trade Unions	Meetings	Potential unlawful processing undertaken under the guise of 'training requirements'	BWC Procedure developed

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.

Personal data shall be obtained only the specified purposes, and shall not be further processed in any manner incompatible with that purpose.

The information is to safeguard Civil Enforcement Officers, Public Protection Officers and members of the public during enforcement operations and to provide good evidence for all parties in the event of complaints or investigations lodged with the Council or any other investigation into incidents, accidents or alleged assaults.

The Council primarily processes personal data from its CCTV network under the UK General Data Protection Regulation (GDPR), Article 6(1)(e) public task. This basis is underpinned by the Health and Safety Act 1974 which requires the Council to protect persons at work against risks to health or safety arising out of or in connection with activities at work.

There is also a raft of legislation supporting the enforcement action being taken which includes but is not limited to:

- Antisocial Behaviour, Crime and Policing Act 2014
- Consumer Credit Acts 1974 and 2006.
- Consumer Protection Act 1987.
- Consumer Protection from Unfair Trading Regulations 2008
- Criminal Justice Acts 1988 and 1991
- Criminal Justice and Police Act 2001
- Environmental Protection Act 1990
- Food Safety Act 1990 **
- Food Safety and Hygiene (England) Regulations 2013 **
- Health and Safety at Work etc Act 1974 **
- Housing Acts 1985 (as amended) , 1996, 1998, and 2004
- Pollution Prevention and Control Act 1999

The Data Protection Act 2018, Part 3 allows Blackpool Council to act as a competent authority (where it has the powers to do so) to process personal data (including special category data) for the prevention, detection or prosecution of criminal offences.

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.

Consultation will be ad hoc as and when required through the direct interactions made between the Public Protection and Enforcement team and members of public who are involved in protection enforcement action / incident investigation proceedings.

Members of public will be verbally informed when the recording function is activated and there will be a corresponding light visible on the device following its activation.

A privacy notice will be present within the Blackpool Council website which will provide details regarding:
Why we collect information
What is our lawful basis
What types of information we collect
Who we share your information with

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 use of BWV supports the aims of the Council's lone working policy and enables the Council to comply with its duty of care towards its employees as required by the Health & Safety Act 1974..

The data is fully controlled by the Council and data is processed by us and shared under certain conditions detailed within the Council's CCTV Code of Practice. Data is shared with authorised investigating bodies/organisations that have approved investigatory powers such as Lancashire Police. The Council maintains an information sharing agreement with the Police.

BWV procedures have been developed and staff have / will be trained. Its use is subject to compliance checks by either internal audit or the information governance team.

Cameras are only switched on when CEO's are undertaking enforcement action.

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

Images and audio will be stored on a designated Council computer, held securely in the dispatch office which are held on secure Council servers.

Unless marked as evidential all recordings are automatically deleted after 31 days. Evidential recordings are retained for a period of up to 2 years.

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)

As detailed above retained for two years where its been authorised by a Manager as its required for investigation.

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?

- No Processors act on behalf Blackpool Council.
- Employees subject to DBS checks with robust contracts/agreements in place.
- Due diligence on cameras and processing system
- Data held on Blackpool Council's IT infrastructure; it currently holds Cyber Essentials Plus, Public Services Network (PSN) and NHS DSPT Accreditation.
- Mandatory training and mentoring on induction for employees and volunteers.
- Regular training refresh for employees and volunteers.
- Robust policies and procedures.
- Stringent approval process in place for data sharing and robust data sharing agreements that specify purposes.
- Compliance audit

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 robust procedures in place to identify and process any complaints or requests under the individual rights contained within the UK GDPR. These include the Data Protection Policy, Right of Access Procedure and Data & Security Breach Incident Management Procedure.

Information is stored on Council ICT maintained secure servers.
Once the information has been uploaded it will be kept securely on a password protected laptop which can only be accessed by authorised personnel.

The use of data by the Police or in court proceedings will be subject to written documented requests which will be signed for by the person receiving the data.

Reasons stated include the following:

The prevention and detection of crime
The prosecution of offenders
The interests of national security

Subject Access Requests (SAR) are received, managed and responded to by the Council's Information Governance Team within the Governance and Partnership Directorate.

Information requested in line with an SAR will be provided in line with a request from Information Governance to the Head of Service and / or the Civil Enforcement Officer Supervisors (x2).

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.

BWV is a useful means for recording evidence and for demonstrating transparency in respect of Council Officers actions when carrying out their statutory duties. Acquisition of personal data is a collateral function of the use of BWV. Such collateral intrusion is dealt with in accordance with prevailing legislation.

BWV video has been shown to have a significant effect on the moderating of behaviour of third parties subject to enforcement action by Council Officers.

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)

Council Camera Code of Practice
Public Protection and Enforcement Body Worn Video Camera Procedure
Public Protection and Enforcement Body Worn Video Privacy Notice

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 UK GDPR/DPA 2018. As the system is processing personal data it is required to comply with data protection legilsation including the seven key principles contained within the UK GDPR which are as follows: • Lawfulness, fairness and transparency • Purpose limitation - SEE MISUSE OF DATA BELOW • Data minimisation • Accuracy • Storage limitation • Integrity and confidentiality (security) - SEE DATA SECURITY BELOW • Accountability Non-compliance may result in harm or distress to individuals and enforcement action by the ICO, financial risk (via the former or claims) and reputational damage.	Remote, possible or probable Possible	Minimal, significant or severe Significant	Low, medium or high Medium
Compliance with the Human Rights Act 1998, including Article 6: the right to a fair trial, Article 8: right to a private and family life and Article 14: protection from discrimination	Possible	Significant	Medium

Non compliance may impede the rights of individuals and legal action against which may result in financial risk and reputational damage			
Compliance with SC Code of Practice and the Protection of Freedoms Act 2012 which requires relevant authorities to have regard to the code when exercising any functions to which the code relates. Non-compliance 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. However, the surveillance camera code is admissible in evidence in any such proceedings.	Possible	Significant	Medium
Compliance with the Regulation of Investigatory Powers Act 2000 which controls and regulates surveillance. Non-compliance can intrude on individuals privacy and the impact the Council's compliance with the Human Right Act. It may result in legal action by individuals, the financial risk/impact this creates and regulatory action by the Office of Surveillance Commissioners	Possible	Significant	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**
Data Security - this includes the loss or unauthorised access of personal data, both intentional and accidental.	Remote, possible or probable Possible	Minimal, significant or severe Significant	Low, medium or high High

Data misuse by employees, volunteers or partner organisations.	Possible	Signficant	Low
Misidentification of perpetrators by operatives.	Possible	Significant	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.

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?**
Targeted use by Officers in situations where there is risk of confrontation.	Reduced	Medium	Yes
Signage/Privacy - cameras clearly visible on Officers uniforms and individuals informed of processing.	Reduced	Medium	Yes
Staffing measures: • Staff checks/vetting proecedures (Police checks and DBS). • Robust contracts with confidentiality clauses. • Operatives are SIA Licensed. • Induction, training and mentoring of Operatives	Reduced	Low	Yes

Options to reduce or eliminate risk	**Effect on risk**	**Residual risk**	**Measure approved?**
Governance arrangements including designated roles, high level working group with accountability and internal audit working stream.	Eliminated reduced accepted Reduced	Low medium high Low	Yes/no Yes
Tedchnical controls such as robust due diligence on cameras and IT Security accreditations such as PSN, Cyber Essentials Plus and DSPT.	Reduced	High	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:	Head of Public Protection and Enforcement	Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by:	Director Community and Environmental Services (Community & Wellbeing)	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:	Penny King, Information Governance Specialist (IGS)	DPO should advise on compliance and whether processing can proceed.
Summary of DPO advice Assessment will be escalated / authorised by Head of Information Governance (Data Protection Officer).		
DPO advice accepted or overruled by: (specify role/title)	Risks mitigaed to an acceptable risk when considering neccessity and proportionaility of processing.	If overruled, you must explain your reasons.
Comments: Accepted		
Consultation responses reviewed by: Service		If your decision departs from individuals' views, you must explain your reasons.

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

Date and version control: 19 May 2020
v.4