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 Public Space CCTV Upgrade

Data controller(s): Blackpool Council - 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)

Public space CCTV is deployed for the purpose of the prevention, detection and prosecution of crime and to combat anti-social behaviour; this may include processing special category and criminal offence data. The same system is used for public safety purposes. By nature the system processes a large volume of personal data.

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)?

Blackpool Council is upgrading its existing public space CCTV system in the spring of 2023. This upgrade includes a shift in technology from analogue cameras to IP networked cameras which will improve the quality of footage available to the Council and its partners. The upgrade also includes an expansion of coverage (but not geographical location) in the town centre.

Blackpool 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 Section 7 of the Crime and Disorder Act 1998 which places a direct responsibility on Council's to combat crime and anti-social behaviour. Section 163 of the Criminal Justice and Public Order Act 1994 empowers Council's to provide CCTV.

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.

[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/

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.

A public space CCTV system acts as deterrent to crime and anti-social behaviour occurring in the first instance. This is because when maintained and operated to a high standard it is a proven tool in the detection and identification of perpetrators.

CCTV is used to tackle common crimes within Blackpool including vehicle crime and shoplifting; the deployment of an effective system improves the general security of the main retail, leisure areas and some parks/green spaces; both in terms of individual personal security and the security of premises and contents. As a popular tourist resort and also a deprived borough by national standards, the town centre is a particular location that suffers high numbers of incidents of crime and anti-social behaviour; this can cause residents and visitors considerable concern.

Anti-social behaviour that happens frequently in the coverage area includes flyposting, begging, illegal street trading, vandalism and drunken behaviour.

A high quality CCTV system can also reduce the time and cost on law enforcement investigating allegations of crime by providing high quality evidence, this increases the likelihood of the prosecution of offenders and providing justice for individuals.

If required a CCTV can system can be an important tool to detect and assist in acts of terrorism, thus supporting national security. Although Blackpool has not been specifically targeted it remains a busy resort and the national threat level set by the Joint Terrorism Analysis Centre remains at substantial that means nationally an attack is likely.

The use of CCTV improves the perception of the public in respect of the safety of resident and visitors, this provides reassurance for those who use public spaces to live, work, study and visit. This supports the economic wellbeing of the town centre by maintaining a high number of visitors to the resort.

Public space CCTV systems can be used to assist in traffic management (not including speed cameras), car park management, crowd management for major events, town centre management, supporting the response to civil emergencies and locating lost individuals including children.

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?

Cameras are set to capture images only and do not capture audio, no facial recognition technology is applied to the footage.

The area of coverage can be broadly described as public spaces in Blackpool, with a large proportion being in town centre and all areas are signed to notify data subject that CCTV is in operation.

The cameras do not target any specific data subject and they capture any data subjects who visit the Blackpool for any purpose; therefore by default not design this will include a proportion of children and vulnerable individuals.

Cameras constantly run 24 hours a day 365 days a year.

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 are in place to reflect routine processing with partner organisations. Blackpool Council regularly share CCTV image with the following organisations:

- Police,
- National Crime Agency and
- Blackpool Business Improvement District (BID).

Footage is shared securely with the Police via the use of NICE's Digital Evidence Management system.

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)
- ☒ ANPR
- ☐ Stand-alone cameras
- ☐ Other (please specify)
- ☐ Body Worn Video
- ☐ Unmanned aerial systems (drones)
- ☐ Redeployable CCTV

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.

- Images are captured by cameras located in the town centre of Blackpool.
- Images transmitted by secure fibre line to be viewed by the CCTV operators (Staff or approved volunteers) at Blackpool Council's CCTV Control Room in live time.
- Data stored on delegated servers held in the secure server room at Blackpool Council's primary Offices.
- Retrospective footage can be accessed via download for specified purposes.
- Requests from partner organisations are processed by CCTV Control Room Manager. Police requests are administered via NICE's Digital Evidence Management system or with a Lancashire Constabulary DP1 form.

• Secure disclosures are made via NICE's Digital Evidence Management system or a password protected CD/DVD.
• Automatic retention and deletion applied to footage which is set at one month or twelve months for retrospectively downloaded footage.

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.

Blackpool Council CCTV 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)

NICE's Digital Evidence Management system or password protected disc if the former is not possible.

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/working groups and email exchanges	Views raised on preferred purposes and locations.	Considered as part of planned implementation of upgraded system.
Elected Members	(Audit and Scrutiny)	Views raised on preferred purposes and locations	Considered as part of planned implementation of upgraded system
Blackpool Business Improvement District (Shopwatch and Pubwatch)	Consulatation Meetings	Views raised on preferred purposes and locations	Considered as part of planned implementation of upgraded system
Police	Consulation Meetings	Views raised on preferred locations and the requirement for quick access to increase effectiveness of prevention and detection of crime.	Implementation and use of NICE's Digital Evidence Management system.
Public	Media Articles (Gazette)	Raise public awareness of the implementation of a new system.	

Consider necessity and proportionality

12. What is your lawful basis for using the surveillance camera system? Explain the rationale for your chosen lawful basis under the relevant data protection legislation. Consider whether you will be processing special categories of data.

The 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 Section 7 of the Crime and Disorder Act 1998 which places a direct responsibility on Council's to combat crime and anti-social behaviour. Section 163 of the Criminal Justice and Public Order Act 1994 empowers Council's to provide CCTV.

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.

We will let people know that we are operating a Public Space CCTV by placing signs in the areas where operational is in place. For the Town Centre system, we will place clear and prominent signage on street furniture such as CCTV Columns. The signage used will:

- Be clearly visible and readable.
- Contain details of the Council as the CCTV 'owner', and the purpose of the system.
- Include contact details, for example telephone number or website address.
- Be of an appropriate size for the context it is in

The Council publishes its full notice on its website in a layered format and this includes the operation its Public Space CCCTV System. The Council's full notice is regularly reviewed to ensure it complies with the requirements of the UK GDPR and the ICO's best practice guidance.

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?

- Completion of this data protection impact assessment (dpia)
- Targeted deployment
- Privacy screens in use to prevent footage from non-public spaces.
- Mandatory SIA 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 audits by internal audit.

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

Automatic retention and deletion applied to footage which is set at one month or in the event of an incident twelve months for retrospectively downloaded footage.

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 above in 15. If shared with the Police or NCA they become the data controller responsible for compliance with storage limitation (retention) principle of the UK GDPR.

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.
- Vetting (Police Level 2 and DBS) of employees and volunteers with robust contracts/agreements in place.
- Due diligence applied on the security of the new CCTV 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 audits.

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 proactively individuals of their rights under the UK GDPR, including signage where processing is undertaken and on the Council's website.

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.

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.

Lighting and increased patrols of Police and BID Officers assist in achieving specified purposes but are not adequate on their own over a large coverage area (a town centre). Therefore they are required to be supplemented and supported by the use of CCTV. Yes, operation requires to be continuous as crime or anti-social behaviour can occur 24 hours a day 365 days a year.

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)

NICE's Digital Evidence Management system contains audit logs of the above. The CCTV function is subject to internal audit.

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	Significant	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 deployment of cameras in areas of high risk (of crime and ASB) and use of privacy screens.	Reduced	Medium	Yes
Signage in areas where cameras are recording to inform individuals of processing which ensures processing is obvert and not covert.	Reduced	Low	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?
High quality system (move to IP networked)n which ensures footage is of clear and perpetrators are less likely to be misidentified.	Eliminated reduced accepted Reduced	Low medium high Medium	Yes/no Yes
Governance arrangements including designated roles, high level working group with accountability and internal audit working stream.	Reduced	Low	Yes
Tedchnical controls such as robust due diligence on new system 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:	Security, CCTV and Civil Enforcement Manager	Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by:	Assistant 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:	Head of Information Governance (Data Protection Officer	DPO should advise on compliance and whether processing can proceed.
Summary of DPO advice Risks mitigated to an acceptable risk when considering necessity and proportionality of processing.		
DPO advice accepted or overruled by: (specify role/title)	Accepted	If overruled, you must explain your reasons.
Comments:		
Consultation responses reviewed by: Project Board		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: DPO		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)
TalboTalbot Square West Street / Market Street Victoria Street / Bank Hey Street Adelaide Street West / Bank Hey Street will be relocated due to Central development Victoria Street / Coronation Street Abingdon Street / Birley Street Church Street / Corporation Street Promenade / Market street Topping Street / Talbot Road Queen St / Abingdon St Albert Road / Central Dr Kings Square Promenade / Chapel Street	Pelco Esprit and Pelco statics	Approx 100	24 hours	CCTV Control Room	Acceptable

Date and version control: 19 May 2020
v.4

Location type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
Albert Road / Coronation Street Corporation Street / Cheapside Promenade / Adelaide Street West Promenade / Capel street East Topping Car Park Church Street / Leopold Grove Cedar Square / Wood Street Topping Street Jct Lytham Road / Waterloo Road Seaside Way / Chapel Street Seaside Way / Central Coach Station Seaside Way / Rigby Road Lonsdale Road Car Park Bloomfield Road / Yeadon Way Waterloo Road Bridge Yeadon Way / South Car Park Lytham Road Bridge					

Date and version control: 19 May 2020
v.4

Location type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
Lonsdale Car Park (Opp. Football Club) Promenade / Queens Square West Street / Market Street George Bankcroft Park Seaside Way / Chapel Street Station Road / Bond Street Rigby Road / Central Drive Clifton Drive / Burlington Road Louis Horrocks Park (Lytham Rd) Promenade / Adelaide Street West Gynn Square Bickerstaffe square Bank Street Car Park Central Drive / Princess St Central Drive / Grasmere Rd Promenade / Lytham Road Talbot Road / Layton Rd Bispham Road / Low Moor Rd					

Date and version control: 19 May 2020
v.4

Location type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
Prom Manchester Square pumpimg station Dickson road / Queens street Bloomfiied Car park Bloomfield Car Park / Claire Street Chepstow Road / Fulwood Ave Dinmore Place Easington Cresent Langdale Place Bispham Village West Street Car park Palatine Road Bethesda square / Central drive South Pier / Prom Promenade / Waterloo road Promenade / St Chads road Edgerton square Top of Blackpool Tower on South side New Larkhill street Sports Barn Gorton street Stanley Park					

Date and version control: 19 May 2020
v.4

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

Date and version control: 19 May 2020
v.4