



PRIVACY IMPACT ASSESSMENT

PRIVACY IMPACT ASSESSMENT

The below form is designed to assist you in carrying out a privacy impact assessment (PIA).

Privacy Impact Assessment screening questions

These questions are intended to help you decide whether a PIA is necessary in the first instance.

Name of Person Responsible Marc Stephenson - Operations Manager

Date of Assessment: 4th September 2017

Review Date: 4th September 2018

Camera location (if applicable) Newport Bridge (South), Tees Bridge Approach Road, Middlesbrough

Camera Number and type (if known) 397 (HikVision)

Camera type (PTZ, Static etc.) Pan, Tilt and Zoom

Is CCTV system covered by ICO registration number? Yes No

 If so, please state Z590889X

Has the Surveillance Camera Code of Practice self-assessment tool been used to assist in completion of this PIA? Yes No

Will this proposed installation be part of an existing CCTV system certified to the Surveillance Camera Code of Practice? Yes No

Checklist

Answering 'yes' to any of the following questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

Introduction of a new surveillance camera system or additional camera (includes static cameras) which can collect new personal information about individuals Yes No

Changing location and/or field of view of an existing camera Yes No

Upgrading cameras which can obtain additional views or enhanced views which may impact on privacy e.g. HD cameras, IR lighting, more powerful lenses, 360 degree cameras Yes No

Introduction of new technology that may affect privacy (e.g. Automatic Number Plate Recognition, Body Worn Video, Automated Recognition Technology, Unmanned Aerial systems (Drones) or similar Yes No

 If so, please state

Using re-deployable cameras (to be completed for every new deployment) Yes No

Installation of the camera results in decisions or action against individuals in ways that can have significant impact on them (this would include, fine, notifying police, patching through images of suspects to police control rooms and Regulation of Investigatory Powers Act 2000 – RIPA) Yes No

Is the information collected about individuals of a kind likely to raise privacy concerns or expectations? For example, criminal records or other information that people would consider particularly private. (Note: may include radio transmissions from the CCTV Control room to store watch and pub watch systems. These regularly mention individuals and their previous convictions which can be heard by members of the public as well as suspect. The risk would need to be identified in the PIA and the solutions addressed.) Yes No

Introduction of Wi-Fi, microwave, GSM, airwave transmission etc. (Is it encrypted?) Yes No

If so, please state

Extending periods of recording Yes No

Upgrade in recording frames per second (increase in image capture) Yes No

Analogue to digital recording Yes No

Where other agencies/organisations are involved in activities where there is potential for privacy to be compromised, e.g. monitoring, handling, processing, sharing data/images etc. Yes No

Any alteration to the way images and data are handled, viewed, processed, disclosed, shared, disposed, retrieved, accessed, stored Yes No

Any other process or use which increases the risk to privacy Yes No

If so, please give details

Does the introduction of a camera system or individual camera increase the risks to the Organisation? E.g. potential non-compliance with data protection or other legislation, legal actions by individuals, etc. Yes No

If you tick 'YES' to any of the above, please complete the following PIA. If in doubt it would be advisable to complete a PIA anyway and inform the system manager of your decision to do so.

Privacy Impact Assessment

1. Identify the need for a PIA

The following are examples of some of the possible aims of the installation/project. If applicable tick one or more of the following aims then briefly explain what the benefits will be to the organisation, individuals and other parties. If there are other aims please detail and explain.

You can refer to other documentation related to the proposed installation or project e.g. Operational Requirement, business case, project proposal, feasibility survey etc.

1.1 Aims

- a. reducing the fear of crime
- b. deterring and preventing crime
- c. assisting in the maintenance of public order and reducing offences
- d. provide high quality evidence which may assist in the detection of crime and the apprehension and prosecution of offenders
- e. protecting property
- f. providing assistance with civil claims
- g. providing assistance with issues relating to public safety and health
- h. providing assistance and reassurance to the public in emergency situations
- i. Assist with traffic management
- j. Recognition of number plates (ANPR)
- k. Other, please specify

1.2 Benefits

Having identified the aims please explain the benefits to Stockton Borough Council, to individuals and to other parties. This could include such things as reduction in crime and offences, reduction in fear of crime, detection of anti-social behaviour etc. The benefits should be capable of being measured and not anecdotal (If you have completed an operational requirement (OR), as recommended, in relation to this PIA please refer to the OR for risk analysis)

The benefit of the system is providing independent evidence to support a number of legitimate legal aims such as the prevention and detection of criminal offences both on the bridge and the surrounding approaches into the area. Historically the site has been subject to a wide range of criminal offences and a secondary purpose of the camera is to protect the property stored on site which includes equipment, plant, vehicles and materials. The location has also been used on a number of occasions by individuals threatening self harm and the final aim of the camera is to detect these incidents as they occur.

1.3 Summarise why the need for a PIA was identified

Completion of the screening questions will assist in identifying the need for a PIA.

Possible needs might include:

- a. Capture of new personal data/images
- b. New or additional locations/areas which have potential for privacy implications
- c. Use of new technology which is capable of capturing enhanced images e.g. BWV, automated recognition, 360 degree views, higher powered equipment, etc
- d. Surveillance camera systems with audio recording capability e.g. BWV
- e. Alteration to the way images and data are handled, viewed, processed, disclosed, shared, disposed, retrieved, accessed, stored
- f. Use of technology which captures vehicle registration numbers (ANPR)
- g. Other, please specify

2. Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows.

2.1 How is information collected?

- | | |
|---|---|
| <input checked="" type="checkbox"/> CCTV camera | <input type="checkbox"/> BWV |
| <input type="checkbox"/> ANPR | <input type="checkbox"/> Unmanned aerial systems (drones) |
| <input type="checkbox"/> Stand-alone cameras | <input type="checkbox"/> Real time monitoring |
| <input type="checkbox"/> Other (please specify) | |

2.2 Does the systems technology enable recording?

- Yes No

Please state where the recording will be undertaken (no need to stipulate address just Local Authority CCTV Control room or on-site would suffice for stand-alone camera or BWV)

The images recorded by the camera will viewed and stored at Stockton on Tees Borough Council Security and Surveillance Centre as an addition to the current system.

Is the recording and associated equipment secure and restricted to authorised person(s)? (Please specify, e.g. in secure control room accessed restricted to authorised personnel)

The recorded images and associated recording equipment are secure within the control room of the building. The building housing the control room was originally built to utilising the specifications of BS 5979 Category 2 - Alarm Receiving Centre British Standards. The building has an electronic gated entrance as well as internal and external CCTV to control access from the site. Access to images is

permitted only to authorised employees, Police for official investigations and other enforcement agencies.

2.3 What type of transmission is used for the installation subject of this PIA (tick multiple options if necessary)

- Fibre optic
- Wireless (please specify below)
- Hard wired (apart from fibre optic, please specify)
- Broadband
- Other (please specify)

The transmission is on a wireless network, which forms part of the wider scheme.

2.4 What security features are there to protect transmission data e.g. encryption (please specify)

Safeguards, including technical, organisation and physical security measures are in place to prevent unauthorised access to, and maintain the integrity of, images and information. The Council hold ISO 27001 certification and has Cabinet Office approval - Public Services Network (PSI).

2.5 Where will the information be collected from?

- Public places (please specify)
- Car parks
- Buildings/premises (external)
- Buildings/premises (internal public areas) (please specify)

The cameras are mounted in the public realm on a main arterial road network in and out of the Borough of Stockton on Tees. There is no realistic belief of a private and family life however this is a new camera location and data will be mainly from vehicles passing the location. Pedestrian footfall in the area is below average.

- Other (please specify)

2.6 From whom/what is the information collected?

- General public in monitored areas (general observation)
- Vehicles
- Target individuals or activities (suspicious persons/incidents)
- Visitors
- Other (please specify)

2.7 Why is the information being collected? (Please refer to additional documentation where available)

- Crime prevention and detection
- Parking enforcement
- Missing person(s)
- Traffic control purposes
- Intelligence
- Other (please specify)

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

- Used by CCTV operators to detect and respond to unlawful activities in real time
- Used by CCTV operators to track and monitor suspicious persons/activity
- Used to search for vulnerable persons
- Used to search for wanted persons
- Used to support post incident investigation by authorised agencies, including judicial system
- Used to provide intelligence for authorised agencies
- Other (please specify)

2.9 How long is footage stored? (please state retention period)

All footage is stored for 31 days before being auto-deleted from the system, with appropriate audit safeguards to ensure this occurs.

2.10 Retention Procedure

- Footage 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)

2.11 With which external agencies/bodies is the information/footage shared?

- Statutory prosecution agencies
- Judicial system
- Data subjects
- Local Government agencies
- Legal representatives
- Other (please specify)

2.12 How is the information disclosed to the authorised agencies

- Only by onsite visiting
- Copies of the footage released to those mentioned above (please specify below how released e.g. sent by post, courier, etc)
- Offsite from remote server
- Other (please specify)

2.13 Is there a written policy specifying the following? (tick multiple boxes if applicable)

- Which agencies are granted access
- How information is disclosed
- How information is handled
- Recipients of information become Data Controllers of the copy disclosed

Are these procedures made public? Yes No

Are there auditing mechanisms? Yes No

If so, please specify what is audited (e.g., disclosure, production, accessed, handled, received, stored information)

The entire data collection, processing, storage, retention and dissemination is audited by the Data Controller as required under the relevant statutory provision and associated guidance and best practice regulations. Further independent auditing undertaken by certified inspectors such as National Security Inspectorate and Surveillance Commissioner.

2.14 Do operating staff receive appropriate training to include the following?

- Legislation issues
- Monitoring, handling, disclosing, storage, deletion of information
- Disciplinary procedures
- Incident procedures
- Limits on system uses
- Other (please specify)

2.15 Do CCTV operators receive ongoing training?

Yes No

2.16 Are there appropriate signs which inform the public when they are in an area covered by surveillance camera systems?

Yes No

3. Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation?

You can use consultation at any stage of the PIA process. It will be necessary to concentrate any consultation into 'privacy issues'.

Note: there are guidelines on consultation for the public sector issued by the Cabinet Office and elsewhere in this guidance.

3.1 Who have you consulted with? (tick multiple options if necessary)

Internal Consultations

- | | |
|--|--|
| <input type="checkbox"/> Data Protection officer | <input checked="" type="checkbox"/> Engineers, developers, designers, installers |
| <input type="checkbox"/> Information Technology | <input type="checkbox"/> Planning |
| <input type="checkbox"/> Procurement | <input type="checkbox"/> Data Processors |
| <input type="checkbox"/> Corporate governance/Compliance | <input checked="" type="checkbox"/> Research, analysts and statisticians |
| <input checked="" type="checkbox"/> Senior management | <input type="checkbox"/> Other (please specify) |

External Consultations (tick multiple options if necessary)

- | | |
|---|---|
| <input type="checkbox"/> General public | <input type="checkbox"/> Local residents |
| <input type="checkbox"/> Business | <input type="checkbox"/> Education establishments |
| <input checked="" type="checkbox"/> Elected Members (Councillors) | <input type="checkbox"/> Other (please specify) |

3.2 How did you undertake the consultation with the above (e.g. focus groups, on-line public survey, public meetings, targeted mail survey, etc)? (please explain)

Conulstation conducted as part of a project focus group into the redevelopment of the wider bridge area with advancements in lighting, design and repair. Elected Members consulted via electronic email as a notification of scheme given limited impact on the general public living in the area.

3.3 Is feedback available to view?

- Yes No

3.4 What feedback did you have and have you acted on it? (please explain or attach results)

4. Identify the privacy and related risks

The below table provides some examples of possible privacy risks related to the use of a CCTV system. Operators can use this list as a starting point; however, not all of these risks may apply to all CCTV systems or all PIAs.

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register. Remember that the aim of a PIA is not to completely eliminate the impact on a privacy risk. The options in dealing with the risks are to eliminate, reduce or simply accept them.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk
Collecting/ exceeding purposes of CCTV system	New surveillance methods may be unjustified intrusion on persons privacy	Non-compliance with Data Protection, Human Rights legislation	Loss of reputation Fines and sanctions
Retention of images/information for longer than necessary	Owner retaining personal images/information longer than necessary	Non-compliance with Data Protection, Human Rights legislation	Loss of reputation Fines and sanctions
Lack of policies and procedures and mechanisms	No public availability of CCTV code of Practice which details how personal data handled, stored, disclosed etc.	Non-compliance with Data Protection, Human Rights legislation	Loss of reputation Fines and sanctions
Lack of signage	Public not made aware that they are entering an area monitored by surveillance system	Non-compliance with Data Protection, Human Rights legislation	Loss of reputation Fines and sanctions

Risk	Approved solution	Approved by