SURVEILLANCE CAMERA COMMISSIONER

PRIVACY IMPACT ASSESSMENT

PRIVACY IMPACT ASSESSMENT

The template below 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.

Camera location (if applicable)	
Camera Number (if known)	
Camera type (PTZ, Static etc.)	

Is CCTV system covered by ICO registration number? ☐ Yes ☐ No

If so, please state

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.

Privacy Impact Assessment Template

This template is an example of how you can record the PIA process and results. You can start to fill in details from the beginning of the project, after the screening questions have identified the need for a PIA.

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 your organisation, 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)

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?

- ☐ CCTV camera
- ☐ BWV
- ☐ ANPR
- ☐ Unmanned aerial systems (drones)
- ☐ Stand-alone cameras
- ☐ Real time monitoring
- ☐ 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)

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)

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)

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

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)
- ☐ 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
- ☐ Traffic control purposes
- ☐ Parking enforcement
- ☐ Intelligence
- ☐ Missing person(s)
- ☐ 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)

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
- ☐ Local Government agencies
- ☐ Judicial system
- ☐ Legal representatives
- ☐ Data subjects
- ☐ 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)

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

- ☐ Data Protection officer
- ☐ Information Technology
- ☐ Procurement
- ☐ Corporate governance/Compliance
- ☐ Senior management
- ☐ Engineers, developers, designers, installers
- ☐ Planning
- ☐ Data Processors
- ☐ Research, analysts and statisticians
- ☐ Other (please specify)

External Consultations (tick multiple options if necessary)

- ☐ General public
- ☐ Business
- ☐ Neighbourhood panels
- ☐ Local residents
- ☐ Education establishments
- ☐ 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)

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

Below are some suggested risks and solutions. Feel free to use some or all of them or some of your own.

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

5. Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Note: please mark any 'privacy by design' solutions with an asterisk *

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Collection of images/information exceeds purposes	Restrict collection of images/information to identified purposes and locations. Implement appropriate technological security measures and document *	Reduced	If the images were reduced to the identified purposes by introducing 'Privacy zones'. The collection of images/ information would be justified, compliant and proportionate
Retention of images/information	Introduce retention periods to only keep information for as long as necessary. These are specified in the publicly available CCTV Codes of Practice.	Reduced	As stated retention periods introduced and specified are justified, compliant and proportionate
Lack of policies and procedures and mechanisms	Produce polices for handling, storage, disclosure of images/information and make them publicly available in the CCTV Codes of Practice.	Eliminated	Relevant policies now available as stated This is now justified, compliant and proportionate
Lack of signage	Gap analysis of area covered by CCTV system to ascertain if there is prominently placed signage at the entrance to the area monitored and also within that area. All signs to be mapped and audited regularly.	Reduced	Gap analysis indicated not enough prominent signs. Now installed an additional 12 signs and also mapped all existing signage. This is now justified, compliant and proportionate

6. Sign off and record the PIA outcomes

This section is for the decision maker in the organisation to sign off each risk. Who has approved the privacy risks involved in the project; what solutions need to be implemented; who and at what level?

The example below shows the information required. You will need to list each identified risk, solution and approved sign off.

Risk	Approved solution	Approved by
Collection of images/ information exceeds purposes	Restrict collection of images/information to identified purposes and locations. Implement appropriate technological security measures and document *	Decision makers' signature Note: the PIA does not always require formal sign-off. However, it would be good practice to ensure that the PIA has been approved at a senior level.